UNIWERSYTET W BIAŁYMSTOKU

WYDZIAŁ PRAWA

Janusz Wasilewski

CYBERPRZESTĘPCZOŚĆ - WYBRANE ASPEKTY PRAWNOKARNE I KRYMINALISTYCZNE

Praca doktorska napisana
w Katedrze Prawa Karnego
pod kierunkiem
dr hab. Ewy M. Guzik-Makaruk, Prof. UwB

BIAŁYSTOK 2017

SPIS TREŚCI

WSTĘP

Nieustanny postęp technologiczny, będący dziś imperatywem o sile nieomal równej postępowi biologicznemu, codziennie zmienia otaczającą nas rzeczywistość kreując nowe możliwości, ale także wyzwania. W szczególności twierdzenie to dotyczy rozwoju nowoczesnych technik komputerowych lub szerzej teleinformatycznych, które będąc jeszcze zaledwie kilkadziesiąt lat temu przedmiotem powieści *science-fiction*, dziś stanowią powszechnie stosowane rozwiązania. Mieszczące się w tym trendzie zjawiska jak bankowość elektroniczna, cyfrowy podpis, nieograniczona terytorialnie wymiana informacji, możliwości zdalnego zarządzania najróżniejszymi zasobami sieciowymi, ale także rozwiązania społecznościowe, czy rozrywkowe prowadzą w efekcie do wirtualizacji rzeczywistości i cyfryzacji ludzkiego życia. Znakiem czasów stało się przetwarzanie w systemach teleinformatycznych jak największych ilości danych o nas samych oraz naszych działaniach.

O ile rozwój technologii urzeczywistnia ideę tzw. globalnej wioski[1], w której pojęcie granic państwowych staje się równie wirtualne, jak ruch sieciowy, a możliwości kooperacji obejmują w istocie cały glob, o tyle nowe, wirtualne obszary ludzkiej aktywności stanowią jednocześnie także nieodkryty grunt dla zupełnie nowych form działalności przestępczej[2]. Tak jak globalne są korzyści wynikające ze stosowania nowych rozwiązań, tak samo globalne są związane z tym zagrożenia, których najgłośniejsze przykłady stanowią ataki hackerskie na Estonię w 2007 r., czy tzw. „Operacja Aurora"[3] (druga połowa 2009 r.) będąca serią niezwykle wyrafinowanych cyberataków, skierowanych przeciwko największym firmom branży IT m.in. koncernowi Google.

Immanentną częścią rzeczywistości wirtualnej, zarysowującą się właściwie już od początku istnienia domeny cyfrowej, było odzwierciedlanie się w niej wszelkich, w tym także negatywnych, przejawów ludzkiej działalności. Prawidłowość ta, z uwagi na wyłącznie

---

1 Pojęcie spopularyzowane przez kanadyjskiego pisarza Marshalla McLuhana, oddaje ideę zbliżania różnych (etnicznie, geograficznie, kulturowo, majątkowo itd.) społeczności dzięki upowszechnianiu obiegu informacji prowadzonemu z wykorzystaniem nowoczesnych technologii teleinformatycznych. Zob. także L. Duff, S. Gardiner, *Compuer Crime in the Global Village: Strategies for Control and Regulation - in Defence of the Hacker*, w: D. S. Wall, *Cyberspace Crim*e, Wyd. Ashgate, Anglia 2003, s. 145 i nast.

2 Jest to jedna z podstawowych, wyjściowych tez wszelkich opracowań dotykających omawianego tematu, m.in. pojawiająca się w amerykańskim raporcie sporządzonym w 2000 r. przez prezydencką grupę roboczą, zatytułowanym *The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet*.

3 Szerzej na ten temat na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Operation_Aurora

rosnące tempo rozwoju technologii, stanowi dziś ogromne wyzwanie praktyczne dla prawa – tak w zakresie jego stosowania (ustalania właściwości, interpretacji, egzekucji prawnej), jak i dla procesu legislacyjnego. Specyfika świata wirtualnego jest na dziś tyle wyraźna, że wymaga odpowiedniego uwzględnienia w obu wskazanych wyżej obszarach funkcjonowania prawa.

Niniejsza praca została poświęcona zagadnieniom zwalczania cyberprzestępczości - czyli tego zakresu czynów bezprawnych, których negatywne przejawy występują w wirtualnym świecie systemów teleinformatycznych. I chociaż istnienie zjawiska cyberprzestępczości stanowi dziś na świecie niepodważalny fakt, zaś jego powszechność w krajach rozwiniętych zaczyna być wręcz oczywista, nie można wyciągnąć bardziej mylnego wniosku od tego, że problem ten został już dostatecznie zbadany i opisany. Wciąż mała, choć powoli rosnąca, liczba opracowań w tym zakresie jest niewystarczająca by stawić czoło nie tylko obecnym, ale tym bardziej nadchodzącym wyzwaniom. Należy oczywiście taki stan zmienić, co jednak z uwagi na niezwykle dynamiczny charakter zjawiska cyberprzestępczości wymagać będzie znacznie szerszego zaangażowania w proces badawczy przedstawicieli wszystkich zawodów prawniczych. Międzynarodowy charakter cyberprzestępczości wymusza z kolei zacieśnienie współpracy państw oraz podejmowanie kolejnych inicjatyw na arenie międzynarodowej w omawianym zakresie.

Dla wykazania potencjalnej skali problemu cyberprzestępczości oraz dalszego jej rozwoju w Polsce należy przede wszystkim zwrócić uwagę na tempo rozwoju kraju w obszarze teleinformatyki. O ile dosyć opóźnione oraz powolne początki komercyjnego dostępu do Internetu w Polsce sięgają dopiero 1993 r., o tyle w roku 1999 szacunkowa liczba użytkowników sieci w kraju przekraczała już jeden milion[4], zaś badania z lat 2008 i 2009 wykazały kolejno, że w latach tych dostęp do Internetu był w odpowiednio 48[5] i 53[6] procentach gospodarstw domowych. Obecnie z Internetu korzysta 2/3 Polaków, z czego 80% przynajmniej raz kupiło coś w sieci, zaś 20% deklaruje, iż w ciągu roku poznało kogoś *on-line*[7]. Liczby te wyraźnie ilustrują dynamikę procesu rozwoju. Ustawicznie rośnie także ilość zastosowań sieci, z których korzystają Polacy. Jak wynika z badań przeprowadzonych w roku 2009 z usług bankowości elektronicznej aktywnie korzystało ponad siedem i pół miliona

---

4 Materiał pochodzący z konferencji „Obywatele Internetu", która odbyła się w Trzebinie 29.06.1999 r., dostępny pod adresem http://www.wsp.krakow.pl/papers/trzebinia.html.

5 Źródło: http://wiadomosci.gazeta.pl/Wiadomosci/1,80353,5108762.html.

6 Źródło: http://www.wirtualnemedia.pl/artykul/67-proc-polskich-gospodarstw-domowych-ma-komputer-ile-korzysta-z-internetu#.

7 Na podstawie: Komunikat z badań CBOS pn. „Internauci 2015".

Polaków, podczas, gdy rok później liczba ta wyraźnie przekraczała już osiem milionów[8]. Liczba osób, które zawarły z bankami umowę o dostęp do rachunku przez Internet kształtowała się natomiast w tych samych latach na poziomie, odpowiednio trzynastu i pół oraz prawie czternastu i pół miliona potencjalnych użytkowników[9]. Obecnie z usług e-bankowości korzysta połowa dorosłych Polaków[10]. Zgodnie z dalszymi prognozami oraz planami rozwoju informatyzacji kraju trend ten nie tylko będzie się utrzymywać, ale w dodatku przybierać na sile. Jako swoisty punkt odniesienia dla dalszego rozwoju można wskazać na statystyki największego portalu społecznościowego – Facebook, z którego na świecie korzysta już ponad pół miliarda osób zaś w samych USA ponad sto czterdzieści milionów użytkowników[11]. W Polsce, na początku 2013 r., zarejestrowanych było prawie dziesięć milionów kont Facebook. Granicą rozwoju informatyzacji w świetle przedstawionych danych wydaje się być dopiero włączenie do omawianego procesu całej ludzkości oraz wszystkich obszarów naszej aktywności, zarówno zawodowej, społecznej, jak i rozrywkowej. Mając przytoczone liczby na uwadze oraz uwzględniając przy tym ciągle pojawiające się nowe rodzaje coraz to niebezpieczniejszych zagrożeń, jak np. robak komputerowy *Stuxnet*[12], który po raz pierwszy w historii zagroził fizycznymi uszkodzeniami infrastruktury krytycznej[13] całego świata, konieczność zapewnienia bezpieczeństwa w cyberprzestrzeni wydaje się być aktualnie jednym z priorytetów, tak w skali poszczególnych obywateli, jak i całych państw, również na poziomie międzynarodowym.

Celem pracy jest dokonanie kompleksowej analizy problemu cyberprzestępczości zarówno w płaszczyźnie prawa karnego materialnego, jak i procesu karnego, co pozwala na jego przedstawienie w ujęciu tak statycznym (opis zagrożeń) jak i dynamicznym (problematyka zwalczania). Swoistym bohaterem pracy stała się cyberprzestrzeń, której szeroka charakterystyka pozwala rzucić właściwe światło na kwestie specyfiki cyberprzestępczości oraz problematyki realizacji czynności procesowych podejmowanych w jej obszarze. W ocenie autora pracy - pominięcie charakterystyki obszaru cyberprzestrzeni, pozbawiłoby tytułową analizę nowych form przestępczości szczególnego kontekstu, w istocie warunkującego specyfikę całego fenomenu cyberprzestępczości.

[8] Dane pochodzące z badań Związku Banków Polskich, dostępne między innymi pod adresami http://prnews.pl/aktualnosci/liczba-aktywnych-klientow-bankowosci-elektronicznej-wynosi-juz-77-mln-44037.html

[9] Dane pochodzące z badań Związku Banków Polskich, op. cit

[10] Komunikat z badań CBOS, op cit.

[11] Strona śledząca statystyki portalu Facebook – *Check Facebook*, znajdująca się pod adresem http://www.checkfacebook.com/.

[12] Więcej na temat na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Stuxnet.

[13] Robak zaatakował m. in systemy elektrowni atomowej w Iranie.

Szczególna charakterystyka zdarzeń karno-prawnych występujących w cyberprzestrzeni stała się w efekcie główną inspiracją niniejszej pracy oraz pozwoliła sformułować jej wstępną tezę, iż faktyczne pojawienie się cyberprzestrzeni - jako specyficznego obszaru ludzkiej aktywności, charakteryzującego się zupełnie inną topografią niż otaczająca nas rzeczywistość *fizyczna*, spowodowało konieczność odczytywania oraz pojmowania na nowo (w nowym kontekście) obowiązujących regulacji prawnych, wpływając tym samym na sposób interpretacji oraz stosowania prawa karnego we współczesnym społeczeństwie informacyjnym. W jego nowym obrazie w miejsce osób fizycznych pojawili się użytkownicy, w zamian przedmiotów – zasoby, zaś przestrzeń zastąpiono logiczną sferą komunikacji cybernetycznej. Wskazywana problematyka wciąż stanowi istotne *novum* wymagając prowadzenia szeroko zakrojonych prac badawczych, w tym w ogromnej mierze prac o charakterze prawnym.

Dla zrealizowania przedstawionego wyżej celu pracy, przyjęto następującą konstrukcję dysertacji: całość została podzielona na trzy podstawowe obszary badawcze poświęcone odpowiednio: 1) charakterystyce obszaru cyberprzestrzeni; 2) fenomenologii cyberprzestępczości (opartej na regulacjach prawa karnego materialnego); oraz 3) problematyce zwalczania cyberprzestępczości ujętej w dynamicznych elementach prawa procesowego. Całość kończy podsumowanie zawierające syntetyczne wnioski oraz postulaty zmian.

Pierwszy z obszarów pracy - poświęcony opisowi cyberprzestrzeni, będącej nowym obszarem ludzkiej działalności, stanowi próbę zderzenia technicznej oraz prawnej charakterystyki domeny cyfrowej. Opracowana kompilacja definicji oraz zasad budowy i funkcjonowania rozległych sieci teleinformatycznych, pozwoliła na zbudowanie właściwego obrazu tego, czym właściwie jest cyberprzestrzeń oraz „gdzie się znajduje", dając kontekst dla dalszych rozważań na temat stosowania prawa wobec specyfiki zjawiska cyberprzestępczości. Przestępczość ta bowiem - jako występująca w domenie cyberprzestrzeni, jest nierozerwalnie powiązana z istotą rzeczywistości cyfrowej, funkcjonującej wyłącznie, jako obszar logiczny, pozbawiony cech naturalnych, fizycznych, czy geograficznych.

Drugi z wymienionych obszarów pracy, o charakterze materialno-prawnym, zawiera opis zjawiska cyberprzestępczości z uwzględnieniem jego szczególnej specyfiki. Omawiana przestępczość zarysowana została na tle specyfiki samego obszaru cyberprzestrzeni, stanowiącego swoisty „teatr" działań przestępców cybernetycznych. Dla bliższego zdefiniowania zjawiska opisane zostały różnice zakresowe występujące pomiędzy różnymi

pojęciami stosowanymi na określenie omawianej gałęzi działalności przestępnej, jak również przybliżono określone wyrażenia techniczne, odwołujące się do ściśle technicznych cech incydentów bezpieczeństwa teleinformatycznego oraz ataków. W części szczegółowej skupiono się na analizie szeregu rodzajów cyberprzestępstw oraz odniesieniu ich do obowiązujących w Polsce regulacji prawnych, co pozwoliło nie tylko na przedstawienie szerokiej analiz zjawiska, ale także na skatalogowanie przesłanek występowania poszczególnych cyberprzestępstw oraz stworzenie pełnego obrazu przedmiotowego fenomenu.

Część prawno-procesowa została poświęcona problematyce wykrywania i ścigania zdefiniowanych wcześniej cyberprzestępstw. Opisane zostały w niej elementy specyficzne dla prowadzenia spraw karnych przeciwko czynom mieszczącym się w tej kategorii przestępstw. Analizie poddana została również problematyka dowodów elektronicznych, stanowiących podstawę prowadzenia spraw przeciwko cyberprzestępcom. Poprawne rozumienie istoty dowodów elektronicznych należy uznawać za stanowiące niezbędny element realizacji zasady swobodnej oceny dowodu oraz warunek *sine qua non* wydania prawidłowego wyroku. W tej części pracy wskazana została wreszcie także problematyka określania zakresu jurysdykcji poszczególnych państw w domenie cyfrowej.

Ostatnia część pracy poświęcona została sformułowaniu wniosków wypływających z wcześniejszych rozważań oraz wyprowadzeniu szeregu postulatów *de lege lata* oraz *de lege ferenda*.

Z uwagi na interdyscyplinarny zakres pracy łączącej w sobie rozważania o charakterze *stricte* prawnym z elementami podstawowej wiedzy informatycznej, ale także dominację języka angielskiego w zakresie tematyki cyberprzestępczości w pracy pojawia się wiele terminów natury technicznej, w tym obcojęzycznych, których wprowadzenie jest jednak niezbędne dla wykorzystania w możliwie najpełniejszym zakresie aktualnego dorobku naukowego, tak prawnego jak i informatycznego w zakresie problematyki zwalczania cyberprzestępczości.

Szczegółowa koncepcja badań

Przedmiotem badań prowadzonych w niniejszej pracy jest problematyka definiowania oraz zwalczania nowoczesnych form przestępczości cybernetycznej, ujęta przede wszystkim przez pryzmat wybranych aspektów prawnych. Mając na uwadze fakt istotnego

zniekształcenia typowych instytucji prawnych na gruncie cyberprzestrzeni, powodowanego szczególną specyfiką tego obszaru, za konieczne uznano przeprowadzenie badań odnoszących się do poprawnego zrozumienia fenomenu przestępczości komputerowej oraz mających na celu w szczególności podwyższenie kompetencji w zakresie kwalifikacji prawnej tak nazwanej grupy czynów zabronionych na gruncie obowiązujących przepisów karnych. Należy zaznaczyć, iż cyberprzestrzeń - będąca nową, cyfrową domeną działalności człowieka, przyniosła nie tylko szereg zupełnie nowych możliwości komunikacyjnych, czy też usługowych, lecz także nieznane dotąd zagrożenia oraz rysujące się na ich tle wyzwania dla organów wymiaru sprawiedliwości odpowiedzialnych za zapobieganie, zwalczanie oraz ściganie przestępstw.

Stan literatury oraz piśmiennictwa krajowego w przedmiotowym zakresie należy oceniać, jako wciąż nie wystarczający do opisu omawianych zjawisk przestępnych, a także specyfiki ich ścigania. Choć liczba artykułów oraz opracowań poruszających tę tematykę wyraźnie wzrosła w ciągu kilku ostatnich lat, analizowane zagadnienia wciąż pozostają tematyką *nowoczesną* oraz niszową. Twierdzenie to powoduje, że odnośne opracowania często przybierają postać wysoce fragmentaryczną, zaś prowadzone rozważania prawnicze najczęściej opierają się wyłącznie na analizie dogmatycznej przepisów, nie wnikając w stronę merytoryczną zjawiska (brak kontekstu faktycznego). Jednocześnie, opracowania tematu starsze niż zaledwie 3-4 lata pozostają obecnie już w dużej mierze nieaktualne z uwagi na zachodzące zmiany zjawiska przestępczości cybernetycznej.

Mając powyższe na uwadze, jako cele badawcze dla niniejszej pracy doktorskiej wyznaczono, w podziale na odcinki badawcze:

1) analizę stanu prawnego oraz dokumentów *quasi*-normatywnych w płaszczyźnie krajowej oraz międzynarodowej w zakresie legalnego definiowania cyberprzestrzeni, ujmowanej jako szczególny obszar aktywności ludzkiej, w tym potencjalne *miejsce* popełniania przestępstw;
2) przybliżenie - w zakresie niezbędnym dla prowadzenia dalszych, szczegółowych rozważań prawniczych, wybranych aspektów technicznych budowy oraz funkcjonowania sieci komputerowych, w szczególności sieci Internet stanowiącej fundament cyberprzestrzeni;
3) analizę stanu prawnego oraz dokumentów *quasi*-normatywnych w płaszczyźnie krajowej oraz międzynarodowej w zakresie legalnego definiowania oraz opisu fenomenu cyberprzestępczości,
4) analizę możliwości przyjęcia nowego podziału cyberprzestępczości z zastosowaniem

kryterium odwołującego się do zasad funkcjonowania cyberprzestrzeni oraz obsługi ruchu sieciowego jej użytkowników;

5) szczegółową analizę cyberprzestępstw o najwyższej doniosłości pragmatycznej prowadzoną w ujęciu zarówno prawnym, jak i merytorycznym (interdyscyplinarny charakter rozważań), realizowaną na podstawie aktów normatywnych krajowych oraz międzynarodowych;
6) ocenę obowiązujących przepisów krajowych pod kątem ich zastosowania do zwalczania przestępczości cybernetycznej, ze szczególnym uwzględnieniem problematyki pozyskiwania dowodów elektronicznych.

Ze względu na prawno-kryminologiczny charakter niniejszej pracy, prowadzone badania realizowane były zarówno w ujęciu dogmatycznym, jak i empirycznym.

Problemy i hipotezy badawcze

Przeprowadzone na potrzeby niniejszej pracy badania pozwoliły na wyodrębnienie następujących ogólnych i szczegółowych problemów badawczych odnoszących się do wymienionych wyżej odcinków badawczych:

Odcinek Nr 1:

A. Problem badawczy ogólny został sformułowany w następujący sposób:

- jak kształtuje się stan prawny oraz *quasi*-normatywny w płaszczyźnie krajowej oraz międzynarodowej w zakresie legalnego definiowania cyberprzestrzeni, ujmowanej jako szczególny obszar aktywności ludzkiej, w tym potencjalne *miejsce* popełniania przestępstw?

B. Problemy badawcze szczegółowe zidentyfikowano w formie poniższych pytań:

- czy w wybranych krajach obowiązują przepisy lub też dokumenty o charakterze *quasi*-normatywnym definiujące zjawisko cyberprzestrzeni?
- czy zidentyfikowane definicje cyberprzestrzeni opisują przedmiotowy obszar w sposób kompleksowy?
- czy zakres przedmiotowy zidentyfikowanych definicji posiada cechy wspólne oraz jakie są ewentualne różnice w sposobie ujmowania cyberprzestrzeni na gruncie różnych porządków prawnych?

- jakie są podstawowe cechy cyberprzestrzeni, jako obszaru definiowanego prawnie?

Odcinek Nr 2:

A. Problem badawczy ogólny został sformułowany w następujący sposób:

- jak warunkowane jest zrozumienie istoty cyberprzestrzeni w odniesieniu do poznania podstawowych aspektów technicznych z zakresu budowy oraz funkcjonowania tego obszaru na poziomie infrastrukturalnym oraz sprzętowo-programowym?

B. Problemy badawcze szczegółowe zidentyfikowano w formie poniższych pytań:

- czy analiza prawna zjawiska cyberprzestrzeni oraz fenomenu cyberprzestępczości może być prowadzona w oderwaniu od prezentacji oraz przybliżenia ich merytorycznych aspektów technicznych?
- czy zrozumienie podstaw technicznych cyberprzestrzeni warunkuje możliwość zrozumienia oraz dalszego opisu zjawiska cyberprzestępczości?
- w jaki sposób poznanie strony technicznej cyberprzestrzeni oraz cyberprzestępczości warunkuje możliwości poprawnej interpretacji, stosowania, a także tworzenia prawa w zakresie zwalczania zagrożeń cybernetycznych?

Odcinek Nr 3:

A. Problem badawczy ogólny został sformułowany w następujący sposób:

- jak kształtuje się stan prawny oraz *quasi*-normatywny w płaszczyźnie krajowej oraz międzynarodowej w zakresie legalnego definiowania cyberprzestępczości?

B. Problemy badawcze szczegółowe zidentyfikowano w formie poniższych pytań:

- czy w wybranych krajach obowiązują przepisy lub też dokumenty o charakterze *quasi*-normatywnym definiujące zjawisko cybeprzestępczości?
- czy zidentyfikowane definicje pojęć stosowanych do opisu omawianej gałęzi czynów zabronionych kształtują ich zakres definicyjny w sposób spójny oraz kompleksowy?
- czy zakres przedmiotowy zidentyfikowanych definicji posiada cechy wspólne oraz jakie są ewentualne różnice w sposobie ujmowania zjawiska cyberprzestępczości na gruncie różnych porządków prawnych?
- jakie są podstawowe cechy cyberprzestępczości?

Odcinek Nr 4:

A. Problem badawczy ogólny został sformułowany w następujący sposób:

- czy powszechnie stosowana typologia przestępczości z zastosowaniem kryterium naruszanego dobra prawnie chronionego jest właściwa dla opisu zjawiska cyberprzestępczości?

B. Problemy badawcze szczegółowe zidentyfikowano w formie poniższych pytań:

- czy cyberprzestępczość, z uwagi na swoje cechy szczególne, warunkowane specyfiką cyberprzestrzeni, poddaje się typologicznemu podziałowi na kategorie przestępstw wyróżniane na podstawie kryterium naruszanego dobra prawnego?
- czy możliwe jest zaproponowanie innego kryterium podziału cyberprzestępczości niż wymienione wyżej?
- czy zastosowanie innego kryterium podziału cyberprzestępczości może przyczynić się do uporządkowania opisu prawnego zjawiska, a tym samym ułatwić jego zrozumienie od strony prawnej?

Odcinek Nr 5:

A. Problem badawczy ogólny został sformułowany w następujący sposób:

- w jaki sposób w obowiązującym stanie prawnym ujmowane są poszczególne typy cyberprzestępstw?

B. Problemy badawcze szczegółowe zidentyfikowano w formie poniższych pytań:

- czy obowiązujący system prawa krajowego dokonuje w sposób poprawny penalizacji przestępstw cybernetycznych?
- czy obowiązujący system prawa karnego penalizuje zjawisko cyberprzestępczości w sposób kompleksowy oraz spójny?
- czy zakres przedmiotowy poszczególnych przestępstw cybernetycznych wyróżnianych na gruncie obowiązującego kodeksu karnego wyczerpuje całokształt przejawów poszczególnych typów czynów bezprawnych?
- jakie są cechy cyberprzestępstw definiowanych na gruncie kodeksu karnego?
- w jaki sposób dokonywać subsumcji poszczególnych rodzajów ataków cybernetycznych do przesłanek formalnych ujętych w poszczególnych przepisach karnych?

- czy krajowy system prawa karnego uwzględnia w swoich przepisach obowiązujące regulacje międzynarodowe? Czy regulacje te zostały poprawnie implementowane do porządku prawnego RP?

Odcinek Nr 6:

A. Problem badawczy ogólny został sformułowany w następujący sposób:

- czy obowiązujące w kraju regulacje karno-procesowe w sposób należyty identyfikują oraz ujmują specyfikę zwalczania przestępczości cybernetycznej, ze szczególnym uwzględnieniem problematyki pozyskiwania dowodów elektronicznych?

B. Problemy badawcze szczegółowe zidentyfikowano w formie poniższych pytań:

- w jaki sposób specyfika cyberprzestrzeni oraz cyberprzestępczości zniekształcają standardowy sposób postrzegania czynności procesowych oraz sposób możliwości ich prowadzenia?
- czy obowiązujący system prawa krajowego pozwala na jednoznaczne opisanie od strony prawnej wszystkich elementów procesu karnego prowadzonego w zakresie postępowań w sprawie o cyberprzestępstwa?
- czy obowiązujący w kraju system prawa karnego procesowego zawiera regulacje poddające się bezpośredniemu oraz pełnemu stosowaniu wobec zwalczania cyberprzestępstw?
- jakie obszary regulacji procesowej pozostają bez należytych rozwiązań prawnych w odniesieniu do prowadzenia czynności procesowych w cyberprzestrzeni, stając się swoistymi lukami prawnymi?
- w jakim zakresie odpowiednie stosowanie przepisów procesowych odnoszących się do realizacji czynności o charakterze konwencjonalnym (przeszukanie, zatrzymanie rzeczy) pozwala na utrzymanie realizacji celów procesu karnego w odniesieniu do zwalczania przestępczości komputerowej?
- jakie są współczesne wyzwania procesu karnego w odniesieniu do zwalczania cyberprzestępczości?

Postawione powyżej problemy badawcze pozwoliły sformułować następujące hipotezy ogólne i szczegółowe, przedstawione z zachowaniem kolejności wyodrębnionych odcinków badawczych.

Odcinek Nr 1:

A. Hipoteza badawcza ogólna została sformułowana w następujący sposób:

- stan prawny oraz *quasi*-normatywny w płaszczyźnie krajowej oraz międzynarodowej w zakresie legalnego definiowania cyberprzestrzeni, ujmowanej jako szczególny teatr aktywności ludzkiej, w tym potencjalne *miejsce* popełniania przestępstw, posiada istotne braki normatywne oraz charakteryzuje się licznymi różnicami powodującymi niekompatybilność poszczególnych systemów prawnych

B. Hipotezy badawcze szczegółowe przyjęły następujące brzmienie:

- w wielu systemach krajowych obowiązują przepisy lub też dokumenty o charakterze *quasi*-normatywnym definiujące zjawisko cyberprzestrzeni,
- zidentyfikowane definicje cyberprzestrzeni opisują przedmiotowy obszar w sposób bardzo zróżnicowany, w wielu przypadkach prowadzący do fragmentaryzacji zakresu przedmiotowego pojęcia,
- zidentyfikowane definicje posiadają elementy wspólne (jak wskazanie na szeroko rozumiane elementy infrastrukturalne, możliwości wymiany informacji, czy też globalny zasięg cyberprzestrzeni), ale daje się także wyodrębnić katalog cech szczególnych pojawiających się na gruncie jedynie wybranych definicji (np. podkreślenie wirtualności obszaru cyberprzestrzeni, wskazanie wprost na rolę użytkowników oraz relacje zachodzące pomiędzy nimi),
- do podstawowych cech cyberprzestrzeni, jako obszaru definiowanego prawnie, należy zaliczyć w szczególności: logiczny charakter przedmiotowego obszaru – rozumiany jako oderwanie samej cyberprzestrzeni od tworzącej ją warstwy infrastruktury technicznej, transgraniczność, wirtualizację występujących w jej obszarze wartości prawnych, wykształcenie nowych, nieznanych poza cyberprzestrzenią usług, wartości prawnych oraz możliwości i wyzwań dla organów ścigania występujących w kontekście cyfryzacji zasobów mogących stanowić tzw. dowody elektroniczne.

Odcinek Nr 2:

A. Hipoteza badawcza ogólna została sformułowana w następujący sposób:

- zrozumienie kwestii prawnych dotyczących szeroko rozumianej regulacji cyberprzestrzeni pozostaje bezpośrednio uwarunkowane procesem poznania

podstawowych aspektów technicznych z zakresu budowy oraz funkcjonowania tego obszaru na poziomie infrastrukturalnym oraz sprzętowo-programowym,

B. Hipotezy badawcze szczegółowe przyjęły następujące brzmienie:

- kompleksowa analiza prawna zjawiska cyberprzestrzeni oraz fenomenu cyberprzestępczości nie powinna być prowadzona w oderwaniu od prezentacji oraz przybliżenia ich merytorycznych aspektów technicznych, jako pozbawiająca tak opracowany temat odniesienia do kwestii faktycznych,
- zrozumienie podstaw technicznych cyberprzestrzeni stanowi niezbędny element rzetelnego opisu zjawiska cyberprzestępczości?
- poznanie strony technicznej cyberprzestrzeni oraz cyberprzestępczości warunkuje możliwości poprawnej interpretacji, stosowania, a także tworzenia prawa w zakresie zwalczania zagrożeń cybernetycznych poprzez uzupełnienie wszelkich odnośnych rozważań prawnych niezbędnym tłem stanowiącym opis faktyczny omawianych zjawisk. Bez niego, prowadzona analiza prawna odrywa się od sfery przedmiotowej rozważań, czyniąc je zupełnie abstrakcyjnymi.

Odcinek Nr 3:

A. Hipoteza badawcza ogólna została sformułowana w następujący sposób:

- stan prawny oraz *quasi*-normatywny w płaszczyźnie krajowej oraz międzynarodowej w zakresie legalnego definiowania cyberprzestępczości zawiera istotne braki legislacyjne.

B. Hipotezy badawcze szczegółowe przyjęły następujące brzmienie:

- tylko w wybranych krajach obowiązują przepisy lub też dokumenty o charakterze *quasi*-normatywnym definiujące zjawisko cybeprzestępczości,
- zidentyfikowane definicje pojęć stosowanych do opisu omawianej gałęzi czynów zabronionych nie kształtują ich zakresu definicyjnego w sposób spójny oraz kompleksowy – pomiędzy definicjami zachodzą istotne różnice gatunkowe, w szczególności brak jest porozumienia w zakresie ujmowania w pojęciu „cyberprzestępczości" tradycyjnych form działalności bezprawnej, dla której cyberprzestrzeń staje się wyłącznie jednym z potencjalnych mediów,
- zakres przedmiotowy zidentyfikowanych definicji posiada zarówno cechy wspólne, jak również istotne różnice w sposobie ujmowania zjawiska cyberprzestępczości – do

różnic należy zaliczyć w szczególności odnoszenie zakresu przedmiotowego omawianego pojęcia wyłącznie do kwestii formalnych lub też do aspektów technicznych *modus operandi* sprawcy przestępstwa cybernetycznego,

- do podstawowych cech cyberprzestępczości należy zaliczyć działanie sprawcy wewnątrz cyberprzestrzeni, podbudowywanej przez szeroko rozumiane systemy teleinformatyczne, kierowanie działania przestępnego przeciwko funkcjonowaniu tych systemów, działanie *de facto* prowadzone za pomocą określonego ruchu sieciowego oraz wydawania poleceń określonego zachowania systemów, pozostawianie śladów w formie cyfrowej, w tym głównie w postaci tzw. logów, dokumentujących pracę poszczególnych systemów.

Odcinek Nr 4:

A. Hipoteza badawcza ogólna została sformułowana w następujący sposób:

- powszechnie stosowana typologia cyberprzestępczości z zastosowaniem kryterium naruszanego dobra prawnie chronionego nie jest właściwa dla opisu zjawiska cyberprzestępczości – jako nie pozwalająca na realny rozdział poszczególnych typów przestępstw,

B. Hipotezy badawcze szczegółowe przyjęły następujące brzmienie:

- cyberprzestępczość, z uwagi na swoje cechy szczególne, warunkowane specyfiką cyberprzestrzeni, poddaje się typologicznemu podziałowi na kategorie przestępstw wyróżniane na podstawie kryterium naruszanego dobra prawnego z istotnymi utrudnieniami – w omawianej gałęzi przestępczości poszczególne typy przestępstw mogą kierować się na naruszenie różnych wartości prawnych w zależności od szczegółowej konfiguracji danego ataku, co w przypadku podziału przestępczości z zastosowaniem kryterium dobra prawnie chronionego powoduje wielokrotne powielanie jednego rodzaju ataku w wielu kategoriach prawnych,
- tak - zaproponowanie innego kryterium podziału cyberprzestępczości niż wymienione wyżej jest możliwe oraz zostało ujęte w niniejszej pracy. Jako kryterium autorskie przyjęto odniesienie danego rodzaju ataku do struktury funkcjonalnej cyberprzestrzeni,
- w ocenie autora niniejszej pracy, zastosowanie autorskiego kryterium podziału cyberprzestępczości może przyczynić się do uporządkowania opisu prawnego

zjawiska, a tym samym ułatwić jego zrozumienie od strony prawnej, pozwalając jednocześnie na usystematyzowanie poszczególnych rodzajów cyberprzestępstw.

Odcinek Nr 5:

A. Hipoteza badawcza ogólna została sformułowana w następujący sposób:

- w obowiązującym stanie prawnym poszczególne typy cyberprzestępstw ujmowane są w sposób niespójny i niekompleksowy, bez wyraźnego rozdziału poszczególnych kategorii przestępstw oraz niezgodnie z regulacjami międzynarodowymi.

B. Hipotezy badawcze szczegółowe przyjęły następujące brzmienie:

- obowiązujący system prawa krajowego nie dokonuje w sposób poprawny penalizacji przestępstw cybernetycznych,
- obowiązujący system prawa karnego nie penalizuje zjawiska cyberprzestępczości w sposób kompleksowy oraz spójny,
- zakres przedmiotowy poszczególnych przestępstw cybernetycznych wyróżnianych na gruncie obowiązującego kodeksu karnego nie wyczerpuje całokształtu przejawów poszczególnych typów czynów bezprawnych,
- z uwagi na brak regulacji definicyjnych, cechy cyberprzestępstw penalizowanych na gruncie kodeksu karnego wymagają rekonstrukcji w oparciu o zasady interpretacji przepisów, w których typizowane są poszczególne cyberprzestępstwa; katalog tak identyfikowanych cech nie pozwala na budowę spójnego obrazu cyberprzestępczości,
- dokonywanie subsumcji poszczególnych rodzajów ataków cybernetycznych do przesłanek formalnych ujętych w poszczególnych przepisach karnych stanowi istotne wyzwanie interpretacyjne z uwagi na fakt iż przesłanki te nie odwołują się do cech technicznych cyberprzestępstw oraz jednocześnie błędnie identyfikują przedmiot poszczególnych działań bezprawnych (w szczególności wskazując na informacje, nie zaś dane),
- krajowy system prawa karnego nie uwzględnia w swoich przepisach w pełnym zakresie obowiązujących regulacji prawa międzynarodowego – implementacja tych regulacji nie została przeprowadzona w pełni poprawnie.

Odcinek Nr 6:

A. Hipoteza badawcza ogólna została sformułowana w następujący sposób:

- obowiązujące w kraju regulacje karno-procesowe nie identyfikują oraz nie ujmują w sposób należyty specyfiki zwalczania przestępczości cybernetycznej, w tym w szczególności pozostawiając istotne braki regulacyjne w zakresie problematyki pozyskiwania dowodów elektronicznych.

B. Hipotezy badawcze szczegółowe przyjęły następujące brzmienie:

- specyfika cyberprzestrzeni oraz cyberprzestępczości w sposób istotny zniekształciła standardowy sposób postrzegania czynności procesowych oraz sposób możliwości ich prowadzenia,
- obowiązujący system prawa krajowego nie pozwala na jednoznaczne opisanie od strony prawnej wszystkich elementów procesu karnego prowadzonego w zakresie postępowań w sprawie o cyberprzestępstwa – w szczególności brak niezbędnych regulacji do określenia charakteru oraz zakresu podstawowych czynności procesowych, jak przeszukanie oraz zatrzymanie rzeczy (danych),
- obowiązujący w kraju system prawa karnego procesowego nie zawiera całokształtu regulacji poddających się bezpośredniemu oraz pełnemu stosowaniu wobec zwalczania cyberprzestępstw,
- regulacje procesowe pozostają w istocie w pełnym zakresie bez należytych rozwiązań prawnych w odniesieniu do prowadzenia czynności procesowych w cyberprzestrzeni, pozostawiając luki prawne w każdym identyfikowanym obszarze normatywnym,
- odpowiednie stosowanie przepisów procesowych odnoszących się do realizacji czynności o charakterze konwencjonalnym (przeszukanie, zatrzymanie rzeczy) w sposób istotny utrudnia utrzymanie realizacji celów procesu karnego w odniesieniu do zwalczania przestępczości komputerowej – nie uwzględniając specyfiki cyberprzestrzeni oraz cyberprzestępczości, opisywane regulacje prawne wymagają ustawicznego stosowania *per analogiam* lub też odpowiednio, nie dając tym samym właściwych narzędzi, dedykowanych do zwalczania nowoczesnych form przestępczości cybernetycznej,
- pośród największych współczesnych wyzwań procesu karnego w odniesieniu do zwalczania cyberprzestępczości należy wskazać na problematykę pozyskiwania dowodów na odległość (*on-line) oraz w* sposób transgraniczny; problematykę pozyskiwania dowodów z danych poddanych procesowi zaszyfrowania oraz kwestie związane z tzw. procesem anonimizacji ruchu sieciowego, utrudniającego dokonywanie atrybucji ataków do ich sprawców.

Z uwagi na interdyscyplinarny charakter pracy, łączący rozważania prawnicze z technicznymi - odnoszącymi się ściśle do specyfiki budowy oraz działania cyberprzestrzeni, a także specyfiki popełniania cyberprzestępstw (szczególny *modus operandi* sprawcy), w prowadzonych badaniach wykorzystano następujące metody badawcze:

1) metodę dogmatyczną;
2) metodę komparatystyczną;
3) metodę analizy piśmiennictwa;
4) metodę badania dokumentów.

W ramach stosowania metody dogmatycznej, dokonywano analizy oraz interpretacji przepisów krajowych oraz międzynarodowych, z zastosowaniem zasad interpretacji językowej (jako podstawowej), ale także systemowej oraz celowościowej (wspomagająco). Analiza przepisów została skupiona wokół regulacji obowiązującego w RP kodeksu karnego oraz kodeksu postępowania karnego. Uzupełniająco, badaniom poddany został także szereg innych ustaw krajowych odnoszących się do wybranych aspektów funkcjonowania sieci telekomunikacyjnych (w szczególności ustawa – Prawo telekomunikacyjne), systemów administracji publicznej (ustawa o informatyzacji podmiotów realizujących zadania publiczne), czy też ochrony wybranych kategorii informacji kluczowych do bezpieczeństwa państwa (np. ustawa o ochronie informacji niejawnych).

W ramach metody komparatystycznej dokonywane były analizy porównawcze krajowego systemu prawnego z wybranymi regulacjami międzynarodowymi, w szczególności zawartymi w przepisach UE, NATO oraz Konwencji Rady Europy o Cyberprzestępczości. Prowadzone w tym zakresie badania miały na celu wykazania podobieństw oraz różnic – w tym błędów implementacyjnych, rozwiązań krajowych na tle prawa międzynarodowego.

W ramach metody analizy piśmiennictwa dokonano przeglądu szeregu opracowań tematu krajowych oraz zagranicznych, celem zgromadzenia niezbędnych opinii fachowych oraz bazy wiedzy potrzebnej do oceny zjawiska cyberprzestrzeni oraz cyberprzestępczości w sposób rzetelny, kompleksowy oraz obiektywny. Zebrane uwagi rozlicznych autorów zostały ujęte w pracy w możliwie szerokim zakresie w sposób istotny podwyższając walor naukowy niniejszego opracowania.

W ramach zastosowania metody badania dokumentów (tzw. *desk research*) analizie poddano wybrane dokumenty analityczne opisujące fenomen cyberprzestrzeni oraz cyberprzestępczości. Dokumenty te – podobnie jak w przypadku analizy piśmiennictwa, pozwoliły na uwzględnienie w pracy wyników badań przeprowadzonych w poruszanym

zakresie przez innych autorów. W szczególności, w zakresie wykorzystania opisywanej metody uwzględniono informacje dotyczące szczególnych cech realizacji czynności procesowych w obszarze domeny cyfrowej.

Z uwagi na interdyscyplinarny charakter niniejszej pracy, w jej treści uwzględniono także zebraną wiedzę merytoryczną, pozwalającą na prowadzenie odnośnych analiz prawnych w sposób możliwie głęboko umocowany w rozważaniach ściśle faktycznych, prezentujących istotę funkcjonowania cyberprzestrzeni oraz *modus operandi* sprawców poszczególnych kategorii przestępstw cybernetycznych.

Rozdział I
Geneza regulacji prawnych w obszarze zapobiegania i zwalczania przestępczości w cyberprzestrzeni

§ 1. Uwagi ogólne

Wszechobecny rozwój technologiczny, który stał się znakiem rozpoznawczym schyłku XX wieku, wprowadził do otaczającej nas rzeczywistości nie tylko szereg zaawansowanych rozwiązań teleinformatycznych, ale, co równie ważne, przyniósł ze sobą także szczególne przeobrażenia cywilizacyjne[14]. Zmienił się nie tylko sposób funkcjonowania naszych społeczeństw, ale także sam ich kształt. Wciąż rozgrywające się na naszych oczach zjawiska, jak postęp w wirtualizacji rzeczywistości, przypisującej realne wartości nierealnym bytom, pojawienie się niespotykanych dotąd możliwości wymiany ogromnych ilości informacji, stanowiących dziś samoistne towary, czy wreszcie faktyczne wytworzenie się obszaru cyberprzestrzeni, będącej zupełnie nowym teatrem działań dla ludzkiej aktywności - by wymienić tylko kilka przykładów - nie mogły przejść niezauważenie, nie dotykając fundamentów, tak gospodarczych, jak i społecznych, naszej rzeczywistości[15]. Ta swoista rewolucja[16], wpływająca niejednokrotnie na podstawowe mechanizmy funkcjonowania społeczeństwa, musiała w tej sytuacji znaleźć swoje odzwierciedlenie naturalnie także w jeszcze jednym obszarze - w obowiązującym prawie[17].

Niezależnie od przyjętego sposobu definiowania prawa, czy to kierując się wykładnikami szkoły naturalnej, pozytywistycznej, czy socjologicznej, podstawową cechą prawa, jako zjawiska kulturowego, jest jego normatywny, abstrakcyjny charakter[18], wprowadzający rozróżnienie pomiędzy zachowaniami pożądanymi a potępianymi w danej społeczności[19]. Przedmiotem prawa są określone wartości[20], które tworzą uporządkowaną

---

[14] M. Castells wskazuje wręcz na istnienie paradygmatu technologii kierującego transformacjami społecznymi, M. Castells, Społeczeństwo sieci, Wydawnictwo Naukowe PWN, Warszawa 2010, s. 102 i nast.

[15] Na skalę przemian uwagę zwracają już od wielu lat specjaliści branży IT, np.: http://www.gartner.com/it/page.jsp?id=493003.

[16] Nazywana w literaturze także Rewolucją Informacyjną, tak np. A. Adamski, Prawo karne komputerowe, Wydawnictwo CH Beck, Warszawa 2000 r., s. XV.

[17] P. Podrecki, Z. Okoń, P. Litwiński, M. Świerczyński, T. Targosz. M. Smycz, D. Kasprzycki, Prawo Internetu, Lexis Nexis, Warszawa 2007, wyd. 2, s. 159 i nast.

[18] T. Chauvin, T. Stawecki, P. Winczorek, Wstęp do prawoznawstwa, C. H. Beck, Warszawa 2011, wyd. 6, s. 166 - 169.

[19] Szerzej o definicjach prawa pisze A. Kojder, Godność i siła prawa, Oficyna Naukowa, Warszawa 2001 r.,

hierarchię wskazując dobra, które podlegają szczególnej ochronie oraz te, które ewentualnie mogą być dla tej ochrony poświęcone[21].

Jak w każdym nowym - niezbadanym i nieuregulowanym jeszcze wycinku rzeczywistości, kształtowanie się specyficznego prawa regulującego funkcjonowanie ludzi w rozległych (ostatecznie globalnych) sieciach teleinformatycznych, stanowiło pierwotnie proces rozproszony charakteryzujący się wysoką dynamiką[22]. W procesie tym, nowe reguły postępowania wyłaniały się pierwotnie jako normy naturalne, wytwarzane w drodze faktycznego ucierania się określonych stosunków społecznych. Przejawiały się one w działaniach użytkowników komputerów i sieci, którzy wchodzili we wzajemne interakcje na płaszczyźnie nowego medium[23], jakim stała się cyberprzestrzeń. Powszechne zastosowanie nowoczesnych rozwiązań teleinformatycznych - głównie komputerów oraz sieci komputerowych, wytworzyło bowiem specyficzną cyfrową przestrzeń dla podejmowania różnych rodzajów czynności, zarówno tych istotnych wyłącznie obyczajowo, społecznie, jak i prawnych[24]. W przestrzeni tej, w chwili jej narodzin pojęcie prawa było jednak równie abstrakcyjne oraz fizycznie nienamacalne, jak sama tkanka nowopowstałej *cyber-rzeczywistości*. Istniejąc jedynie *wirtualnie* rzeczywistość ta uzyskała specyficzne cechy, dzięki którym szybko stała się niezwykle istotnym polem dla ludzkiej aktywności, na którym nieznane są fizyczne wymiary ani limity geograficzne[25]. Pierwszym przejawem oddolnej regulacji cyberprzestrzeni stała się tzw. *netykieta*[26] - będąca zbiorem podstawowych reguł, jakie obowiązują w sieci. Zawarte w niej są zasady tak trywialne, jak zakaz nadużywania wielkich liter (uważanych za „krzyczące"), oraz tak istotne, jak zakaz nagabywania innych użytkowników natrętnymi wpisami lub mailami (tzw. *cyberstalking*), zakaz zalewania forów internetowych wiadomościami powodującymi dysfunkcję forum (*flooding*), czy wreszcie zakaz rozsyłania *spamu*, czyli niezamawianych informacji, w tym reklam (ten ostatni

---

s. 207 i nast.

20 T. Stawecki, P. Winczorek, Wstęp do prawoznawstwa, Wydawnictwo CH Beck, Warszawa 2003 r., s. 25 i nast.

21 G. Maroń, Zasady prawa. Pojmowanie i typologie a rola w wykładni prawa i orzecznictwie konstytucyjnym, Wyd. Ars boni et aequi, Poznań 2011, s. 122 i nast.

22 Więcej na temat tzw. „cybernetyki społecznej" w: J. Jankowski, Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa, Difin, Warszawa 2012, s. 159 i nast.

23 Pierwotnie poprzez składanie oświadczeń woli w formie elektronicznej, które podpisywane są tzw. podpisem elektronicznym. Szerzej o nich w P. Polański, Prawo Internetu, C. H. Beck, Warszawa 2008, s. XXIII i nast.

24 J. Jankowski, *Technological Destabilization of Law* w: W. Cyrul, *Information Technology of Law*, Wyd. Uniwersytetu Jagiellońskiego, Kraków 2014, s. 15 i nast. oraz s. 21 i nast.

25 D. R. Johnson, D. G. Post, *Law And Borders: The Rise of Law in Cyberspace*, 48 Stanford Law Review 1367 (1996), dostępny na stronie internetowej pod adresem: http://cyber.law.harvard.edu/is02/readings/johnson-post.html.

26 Słowo *netykieta* powstało z połączenia dwóch wyrazów: *net* – sieć oraz *etiquette* - etykieta. Więcej na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Netykieta.

doczekał się swojej formalnej kodyfikacji dopiero kilka lat po tym, gdy był już na dobre częścią nieformalnej *netykiety*). O ile oczywiście szereg zasad wynikających z powszechnie obowiązującego prawa można było zastosować od razu także do regulowania niektórych działań podejmowanych *on-line* przy wykorzystaniu komputerów oraz rozległej infrastruktury sieciowej (np. ogólne zasady odpowiedzialności)[27], o tyle analizowana sfera stworzyła tak wiele zupełnie nowych możliwości oraz - z uwagi na swoją specyfikę - tak istotnie odkształciła sposób dokonywania lub pojmowania dziesiątek znanych, typowych czynności, że w efekcie stała się przestrzenią wymagającą wytworzenia zupełnie nowych, specjalnych uregulowań normatywnych[28].

Część z nich mogła oprzeć się na już wykształconych zasadach sieciowej etykiety, większość jednak musiała dopiero określić obowiązujący kształt nowych realiów, co z uwagi na przyjęte zasady prawne, w szczególności dotyczy regulacji karnych. Niektóre z wykorzystywanych w sieci rozwiązań, jak np. podpis elektroniczny, który zrównany jest w skutkach z podpisem odręcznym, mogły wręcz zaistnieć dopiero po przyjęciu odpowiednich przepisów. Zarówno prawo cywilne, administracyjne, jak i karne musiały zatem zmierzyć się z nowymi wyzwaniami, jakie przyniosły możliwości dokonywania transakcji za pośrednictwem Internetu, podejmowania urzędowych czynności w ramach usług e-administracji, czy popełniania przestępstw, dla których zarówno *corpus delicti*, jak i miejsce zbrodni stanowią w istocie przetwarzane cyfrowo impulsy elektryczne, biegnące po obwodach infrastruktury teleinformatycznej. Procesy te dały początek tworzeniu nowej gałęzi prawa nazywanej w najszerszym ujęciu *prawem komputerowym*. Dziedzina ta, wciąż nie mając ściśle określonych granic, dotyka wszelkich elementów rozległej problematyki cyfrowego przetwarzania danych (informacji) z użyciem komputerów. Pojawiające się w historii informatyzacji głosy podnoszące, że przestrzeń cyfrowa, a w szczególności Internet, powinny pozostać miejscem wolnym od regulacji normatywnych (tzw. internetowa anarchia)[29], potraktowane zostały przez społeczeństwo międzynarodowe, jako swojego rodzaju egzotyka, nie zaś realny postulat wart szerszej analizy[30]. Od cyberanarchii należy odróżnić nurt tzw. *hacktywizmu*, stanowiącego rodzaj wyrazu nieposłuszeństwa

---

27 R. Grabowski, Wpływ Internetu na ewolucję państwa i prawa, praca pod red. R. Grabowskiego, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2008, s. 60.

28 Tak np. J. Jankowski, *Technological Destabilization...,* op. cit., s. 15.

29 Jak zwraca uwagę R. Grabowski liczne grupy internautów przez długi czas uważały wręcz, że Internet jest pozbawiony jakiejkolwiek jurysdykcji pozostając zupełnie wolnym od prawa obszarem. Tak w: R. Grabowski, Wpływ Internetu ..., op. cit., s. 53.

30 Można zauważyć, że państwa wręcz wskazują na konieczność coraz mocniejszego regulowania funkcjonowania Internetu, np.: http://news.ninemsn.com.au/national/1034842/internet-without-laws-a-recipe-for-anarchy

obywatelskiego[31].

Tworzenie prawa to proces polegający w istocie na wyważaniu interesów prawnych[32]. Z powyższego twierdzenia wynikają dwa postulaty, które musi spełniać racjonalne prawodawstwo: po pierwsze, konieczna jest poprawna identyfikacja dóbr, jakie występują w danych stosunkach społecznych, oraz po drugie, niezbędne dla podjęcia jakichkolwiek działań prawodawczych jest ustalenie rzeczywistej potrzeby dokonania odgórnej ingerencji w daną sferę życia obywateli poprzez ustanowienie określonych norm prawnych (sankcjonowanych). Zapewnienie ochrony jednej grupie dóbr często z konieczności logicznej, wiąże się z automatycznym ograniczaniem ochrony dla innych – przykładowo, szerokie prawo do prywatności musi ograniczać swobodę pozyskiwania oraz rozpowszechniania informacji, będącej z kolei filarem wolności słowa.

Niezbędne stąd przy stanowieniu prawa jest ostrożne wyznaczanie wspólnych granic ochrony poszczególnych wartości. W przypadku kształtowania regulacji normatywnych rządzących prawami globalnych sieci komputerowych oraz telekomunikacyjnych, podstawowym przedmiotem takiego konfliktu wartości od początku była kwestia nadzoru nad sieciową aktywnością obywateli. Jego istotą było wyznaczenie granic pomiędzy zakresem realizacji gwarantowanych na poziomie konstytucyjnym praw i wolności, a koniecznością podejmowania przez administrację kontroli działań obywateli, która z jednej strony stanowi środek ochrony tych praw i wolności (w przypadku naruszeń moich praw ze strony innych użytkowników), ale z drugiej, jest także ewentualnym narzędziem represji - *vide* rozwiązania techniczne przyjęte w Chinach, umożliwiające pełną regulację „zagranicznego” ruchu sieciowego[33]. Niezwykle cienka, a czasami wręcz iluzoryczna granica dzieli bowiem niezbędną ochronę od cenzury[34]. Powyższy konflikt nabrał tak zasadniczego znaczenia z uwagi na budowę Internetu dającą potencjalnie nieograniczone możliwości inwigilacji poczynań w sieci, pozwalając na dokładne śledzenie każdego ruchu jej użytkowników. Istotne z tej perspektywy widzenia jest, aby w trakcie analizy obowiązujących oraz projektowanych

---

31 Por. M. Pomarański, Haktywizm jako ruch protestu XXI wieku, w: M. Marczewska-Rytko, Haktywizm. Cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja, Wyd. UMCS, Lublin 2014, s. 159 i nast.

32 M. Kelman, *A Guide to Critical Legal Studies, Harvard University Press*, Londyn 1987, s. 65 i nast.

33 Np. *Golden Shield Project,* nazywany też z angielskiego ironicznie *The Great Firewall of China* (połączenie angielskiej nazwy Wielkiego Muru z terminem *Zapora ogniowa* oznaczającym w języku informatycznym rozwiązanie programowe lub techniczne kontrolujące lub ograniczające ruch sieciowy), czy oprogramowanie *Green Dam*, które od lipca 2009 r. musi być zainstalowane na każdym komputerze – jego zadaniem jest zapisywanie działań użytkownika dla umożliwienia realizacji pełnej kontroli ze strony państwa.

34 Na problematykę tę zwraca uwagę m. in. A.Lach w: Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia teoretyczne i praktyczne, *e-biuletyn* CBKE 2/2004, Wrocław 2004, s. 1. Tekst opracowania dostępny jest na stronie internetowej pod adresem: http://www.bibliotekacyfrowa.pl/Content/24720/Dowody_cyfrowe_w_postepowan.pdf.

regulacji dotyczących funkcjonowania cyberprzestrzeni takie konflikty wartości, ale także sam sposób określania występujących w tej sferze dóbr wymagających ochrony prawnej, rozpatrywać na tle szczególnych właściwości ich elektronicznego środowiska, kształtującego wręcz określoną specyfikę samego pojęcia dobra prawnego[35]. Warto podkreślić, że problematyka ta wprowadza szczególne wyzwania dla procesu tworzenia regulacji karnych materialnych oraz procesowych nakierowanych na zwalczanie przestępczości komputerowej oraz tych związanych z zagadnieniami podejmowania nowoczesnych form czynności operacyjno-rozpoznawczych (m.in. zdalne instalowanie tzw. trojanów – programów pozwalających na niejawne przejęcie kontroli nad komputerem, w tym przypadku w celu pozyskiwania i utrwalania dowodów działalności przestępczej).

Tak jak każda dziedzina regulacji prawnej, analizowany system norm określający reguły postępowania w „wirtualnej rzeczywistości", mógł pojawić się wyłącznie dzięki „zaludnieniu" nowych cyfrowych przestrzeni zgodnie z zasadą, że prawo pojawia się tylko tam, gdzie mamy do czynienia z funkcjonowaniem określonej grupy społecznej[36]. W tym świetle, niezwykle istotne jest by prowadząc rozważania dotyczące prawnych aspektów funkcjonowania cyberprzestrzeni, nie tracić z pola widzenia także szerszego kontekstu, w jakim prawo to funkcjonuje. „Uczestniczenie w cyberprzestrzeni" powinno być przedmiotem zainteresowania przedstawicieli wszelkich nauk humanistycznych, społecznych oraz cybernetycznych, zaś refleksja naukowa nie może pomijać podstaw wiedzy o rozwoju człowieka, jego zachowaniach, czy emocjach, które towarzyszą mu także w tym osobliwym obszarze[37]. Należy bowiem mieć na uwadze, że społeczeństwo informacyjne[38] to nowa społeczna i technologiczna infrastruktura wraz z nowymi, sieciowymi współzależnościami struktur społecznych[39]. Ta interdyscyplinarność w poruszanym zakresie jest szczególnie istotna zważywszy na dokonujące się zacieranie granic pomiędzy światami rzeczywistym

---

35 M. Geist, *Is There a There There? Toward greater certainty for Internet Jurisdiction*, tekst opracowania dostępny na stronie internetowej pod adresem: http://www.law.berkeley.edu/journals/btlj/articles/vol16/geist/geist.pdf.

36 T. Stawecki, P. Winczorek, op. cit., s. 9 i nast.

37 J. Bednarek, Teoretyczne i metodologiczne podstawy badań nad człowiekiem w cyberprzestrzeni, Cyberświat: możliwości i zagrożenia, pod red.: J. Bednarek, A. Andrzejewska, Wydawnictwo Akademickie Żak, Warszawa 2009 r., s. 24 i nast.

38 Termin ten zaproponował jeszcze w latach sześćdziesiątych XX w. japoński ekonomista Tadeo Umesao na opisanie społeczeństwa Japonii, jako społeczeństwa, w którym o standardach gospodarki zaczęły decydować informacja i technologia. Za: A. Kania, Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni, *e-biuletyn* CBKE 1/2009, Wrocław 2009, s. 1. Tekst opracowania dostępny jest na stronie internetowej pod adresem: http://bibliotekacyfrowa.pl/Content/34350/Oszustwo_komputerowe.pdf.

39 K. Doktorowicz, Europejski model społeczeństwa informacyjnego. Polityczna strategia Unii Europejskiej w kontekście globalnych problemów wieku informacji, Wyd. Uniwersytetu Śląskiego, Katowice 2005, s. 23, powtarzam za: A. Suchorzewska, Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem, Oficyna a Wolters Kluwer Business, Warszawa 2010, s. 25.

a wirtualnym, które zaczynają wzajemnie się przenikać, oddziaływując na siebie w obydwu kierunkach[40]. Poruszanie się w sieciach komputerowych to dziś już nie tylko dokonywanie codziennych czynności tyle, że na odległość, głównie za pośrednictwem Internetu, lecz nowa jakość w funkcjonowaniu człowieka, jako cząstki społeczeństwa. Zmiany technologiczne być może stanowią obecnie najsilniejszy czynnik kształtujący nasze realia.

Powyższa problematyka zwracająca uwagę na aspekty około-prawne ma istotne znaczenie dla poprawnego zrozumienia całego tematu. Prawo, będące przecież regulatorem rzeczywistości, z konieczności logicznej nie może się od tej rzeczywistości oderwać i jako takie nie powinno być przedmiotem badań jedynie abstrakcyjnych, odchodzących od regulowanej materii[41]. Badanie prawa nie spełniające wskazanego postulatu traci swój rzeczywisty walor poznawczy. W tych częściach pracy, gdzie rozszerzenie kontekstu prawnego o elementy wkraczające na obszary zagadnień o charakterze etycznym stanowi istotne uzupełnienie prowadzonych rozważań merytorycznych dotyczących poprawnego tworzenia oraz rozumienia przepisów, starano się wprowadzać stosowne odniesienia również do tych kwestii. Kształtowanie prawa w nowym obszarze regulacji pozwala bowiem na potraktowanie go jako swoistego laboratorium badań, umożliwiającego opisywanie określonych zjawisk w ujęciu dynamicznym, w miarę ich powstawania i rozwoju, skutkując nie tylko analizą tego, co jest, ale także tego, co się zmienia, a w efekcie - tego, co może zaistnieć[42]. Możliwości rozwoju regulacji cyberprzestrzeni są zaś równie wirtualne – a co za tym idzie nieograniczone, jak ona sama[43].

§ 2. Geneza regulacji

Przechodząc do ujęcia historycznego należy zaznaczyć, że kształtowanie się regulacji karnych cyberprzestrzeni jest procesem nadal aktualnym, toczącym się cały czas na naszych oczach. Zarówno bowiem kwestia prawnego badania oraz definiowania cyberprzestrzeni, jak i kodyfikowania regulacji nakierowanych na zwalczanie cyberprzestępstw, stanowią zagadnienia występujące nie tylko w najświeższej historii, ale przede wszystkim obecne dziś, konstytuując przedmiot licznych debat zarówno międzynarodowych, jak i krajowych. O ile rozważania dotyczące kwestii aktualnych umieszczone zostały we właściwych rozdziałach

[40] J. Bednarek, op. cit., s. 25.

[41] E. Kozerska, P. Sadowski, A. Szymański, Ze studiów nad tradycją prawa, Difin, Warszawa 2012, s. 251.

[42] Uzupełniająco na temat dyferencjacji, czy prawo się tworzy, czy odkrywa: R. Kevelson, *The Law as a System of Signs, Plenum Press,* Nowy Jork 1988, s. 215 i nast.

[43] N. Takemura, *Crime-and-Punishment-Related Information and Its Control in Postmodern Society: Fundamental Understanding on Control Mode of Information*, w: Przegląd Policyjny Nr 1 (61) 2001 r., s. 18 i nast.

merytorycznych niniejszej pracy, o tyle przedstawione poniżej ujęcie historyczne pozwala na prześledzenie drogi prowadzącej do wytworzenia współczesnego pojęcia cyberprzestrzeni oraz cyberprzestępstwa.

Początki kształtowania się regulacji prawnych obejmujących swoim zakresem przedmiotowym zagadnienia wykorzystywania komputerów oraz sieci teleinformatycznych do podejmowania czynności mających znaczenie prawne (prawnie relewantnych), pozostają w ścisłym związku z procesem tzw. rewolucji informacyjnej[44]. Efektem tej rewolucji stało się przypisywanie informacjom określonych wartości majątkowych, nadając im tym samym charakter towaru. Przyjmując zaproponowany przez A. Adamskiego[45] podział czasowy, owa rewolucja na dobre rozpętała się w latach siedemdziesiątych ubiegłego stulecia, obejmując w pierwszej kolejności najbardziej rozwinięte gospodarczo kraje świata. Wówczas to właśnie rozpoczęła się pierwsza fala reform mających na celu wprowadzenie nowych idei do porządku prawnego. Z przyczyn naturalnych, nowotworzone prawo dotyczyło w największej mierze przetwarzania danych wrażliwych przy użyciu komputerów, gdyż to właśnie ich niezwykłe możliwości obliczeniowe, stanowiły bezpośrednią przyczynę nadchodzącej rewolucji informacyjnej. Wraz z tymi możliwościami wiązały się jednak ogromne zagrożenia, głównie dla prywatności[46], którym należało zapobiec poprzez wprowadzenie stosownych regulacji prawnych[47]. Pierwszym wyrazem kształtowania się nowej dziedziny prawa, nazywanej także *ius informationis*, stały się działania podjęte przez ustawodawstwo Szwecji, które w 1973 r. wprowadziło w życie pierwszą na świecie ustawę o ochronie danych osobowych[48] oraz dostrzegło szereg zagrożeń nadciągających wraz z komputeryzacją.

Przełom lat siedemdziesiątych oraz osiemdziesiątych ubiegłego stulecia przyniósł nowy kierunek regulacji, kiedy coraz powszechniejsze stawało się popełnianie przestępstw związanych z procesami elektronicznego przetwarzania informacji. Chociaż pierwsze doniesienia o tego typu czynach pojawiły się w Stanach Zjednoczonych jeszcze w latach sześćdziesiątych XX w., a dotyczyły piractwa oraz szpiegostwa[49], to jednak dopiero lata osiemdziesiąte stały się świadkiem jednych z najgłośniejszych w historii włamań komputerowych, w efekcie których dokonywano kradzieży na sumy wynoszące dziesiątki

44 A. Kania, op. cit., s. 2.
45 A. Adamski, Prawo karne komputerowe, CH Beck, Warszawa 2000, s. XVI.
46 Na problematykę tę uwagę zwraca m. in. J. Misztal-Konecka, G. Tylec, Ewolucja prawa polskiego pod wpływem technologii informatycznych, Wydawnictwo KUL, Lublin 2012, s. 55 oraz 63 i nast.
47 Należy zauważyć, iż bezpieczeństwo to w istocie jedno z najważniejszych praw człowieka i obywatela. Więcej na ten temat: J. Potrzeszcz, Bezpieczeństwo prawne z perspektywy filozofii prawa, Wydawnictwo KUL, Lublin 2013, s. 46 i nast. oraz s. 82 i nast.
48 A. Adamski, op. cit., s. XVI i nast.
49 A. Bequai, *Technocrimes*, Lexington Mass. 1987, s. 52, cyt. za A. Adamskim, op. cit., s. 1.

milionów dolarów. Lata osiemdziesiąte dały początek także innemu, powszechnemu dziś zjawisku szerokiego rozprzestrzeniania się oprogramowania złośliwego, kiedy w listopadzie 1988 r. Robert Morris, ówczesny doktorant amerykańskiego Uniwersytetu Cornella (*nota bene* syn szefa informatyków NSA[50], a aktualnie profesor *Massachusetts Institute of Technology*) wpuścił do Internetu samoreplikujący się program o nazwie *Creeper*[51] mający na celu policzenie podłączonych do sieci komputerów, wywołujący niezamierzony skutek uboczny w postaci drastycznego obniżenia wydajności systemu, na którym się zainstalował – aż do jego sparaliżowania[52]. W reakcji na szybko rozwijające się zagrożenie, regulacje normatywne mające za zadanie ochronę praw odnoszących się do informacji przetwarzanych w postaci elektronicznej, w tym przede wszystkim regulacje karne różnych państw zaczęły być rozszerzane o nowe typy przestępstw. Zaczęto wówczas wyróżniać kategorię przestępstw komputerowych rozumianych jako te czyny zabronione, które popełniane są przy wykorzystaniu komputera stanowiącego narzędzie do wykonywania nielegalnych cyfrowych operacji na danych przetwarzanych w systemach teleinformatycznych. Ściganie przestępstw zaliczających się do tej kategorii czynów w oparciu o obowiązujące do tej pory przepisy stworzone z myślą o zwalczaniu typowych czynów zabronionych, okazywało się w praktyce wielokrotnie nieskuteczne lub wręcz niemożliwe[53]. Odpowiednie zmiany dotyczące regulacji nowoczesnych form przestępczości pojawiły się w pierwszej kolejności w 1978 r. w ustawodawstwie stanowym USA (rozpoczęła Floryda) oraz we Włoszech, zaś następnie, już w latach osiemdziesiątych i dziewięćdziesiątych, kolejno między innymi w Wielkiej Brytanii, Australii, ustawodawstwie federalnym USA, Kanadzie, Danii, RFN, Szwecji, Austrii, Japonii, Norwegii, Francji, NRD i Grecji[54].

Pierwsza na świecie próba stworzenia jednolitej, spójnej regulacji mającej na celu szczegółowe ujęcie zagadnień zwalczania przestępczości komputerowej podjęta została w amerykańskim Senacie w 1976 r., po tym jak w Komitecie Spraw Rządowych odbyła się

---

50 *National Security Agency.* W tłumaczeniu: Agencja Bezpieczeństwa Narodowego. Jedna z kluczowych, federalnych instytucji USA, zajmująca się m. in. nasłuchem elektronicznym oraz rozwojem nowoczesnych technologii. Więcej na temat NSA na oficjalnej stronie internetowej agencji, dostępnej pod adresem: http://www.nsa.gov/.

51 Z ang. pełzacz; *Creeper*, nazywany także *Robakiem Morrisa*, uważany jest za pierwszego wypuszczonego do sieci robaka komputerowego (rodzaj złośliwego programu podobnego w działaniu do wirusa komputerowego), więcej na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Robak_Morrisa.

52 Więcej na ten temat na stronach internetowych: http://pl.wikipedia.org/wiki/Robert_Tappan_Morris oraz na portalu onet.pl, dział Technowinki, wpis z 17 maja 2011 r. (źródło: Guardian).

53 R. M. Kadir, *The Scope and the Nature of Computer Crimes Statutes - A Critical Comparative Study*, s. 609 I nast. Opracowanie dostępne na stronie internetowej pod adresem: http://www.germanlawjournal.com/index.php?pageID=11&artID=1259.

54 M. Goodman, S. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, s. 34. Opracowanie dostępne na stronie internetowej pod adresem: http://ijlit.oxfordjournals.org/content/10/2/139.citation.

debata nad zasadnością wprowadzenia nowych przepisów adresujących kwestie zwalczania nowoczesnych form przestępczości. Efektem podjętej wówczas inicjatywy stał się wydany w kolejnym roku projekt aktu zatytułowanego *Federal Computer Systems Protection Act* stworzony przez senacki komitet, któremu przewodniczył Abe Ribicoff. Późniejszy wiceprezydent USA, senator Joe Biden, komentując wówczas projekt wskazał na jego ogromne znaczenie dla dalszych losów walki z przestępczością *przyszłości*[55]. Projekt, choć ostatecznie nie został przyjęty (odrzucono go w trakcie dalszych prac w 1979 r.), stał się istotnym punktem wyjścia do podjęcia szerszej dyskusji nad koniecznością uzupełnienia krajowego porządku prawnego w analizowanym zakresie. Pośrednio przyczynił się także do wydania federalnej ustawy *Counterfeit Access Device and Computer Fraud and Abuse Act* z 1984 r., będącej jednym z pierwszych aktów stworzonych specjalnie do walki z przestępczością komputerową. Ustawa ta, wprowadzając karalność szeregu *cyberprzestępstw* (*cybercrime*), w tym w szczególności skierowanych przeciwko krajowym systemom teleinformatycznym, stała się w USA podstawowym narzędziem walki z tą formą przestępczości i choć z pewnymi poprawkami, obowiązuje do dnia dzisiejszego.

Nieco innym torem poszła początkowo legislacja Wielkiej Brytanii, gdzie pierwotnie próbowano uzupełniać ogólne regulacje karne, dotyczące typowych czynów zabronionych, rozwiązaniami specyficznymi dla zwalczania nowoczesnej cyberprzestępczości. Dokonana w tym zakresie implementacja szybko okazała się jednak niewystarczająca, czego dowodem były liczne porażki angielskiego wymiaru sprawiedliwości niezdolnego do walki z przestępczością komputerową. Mocnym impulsem do wznowienia prac legislacyjnych mających naprawić ten stan rzeczy stała się sprawa Roberta Schifreen'a[56], który po zatrzymaniu za włamanie się do systemu teleinformatycznego operatora telefonii British Telecom (BT) został uniewinniony z powodu niemożności skazania go na podstawie regulacji przyjętych w ustawie z 1981 r. *Forgery and Counterfeiting Act*[57].

Ustawa ta odnosząc się do kwestii nowoczesnych form przestępczości m. in. poprzez definicję „instrumentu" obejmującą również elektroniczne nośniki informacji, okazała się jednak nie ujmować w sposób dostateczny specyfiki przestępstw komputerowych, których opis faktyczny nie zawsze pozwalał na dokonanie subsumcji pod przepisy stanowiące

---

[55] S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, s. 3. Opracowanie dostępne na stronie internetowej pod adresem: www.cybercrimelaw.net/documents/cybercrime_history.pdf.

[56] Więcej na ten temat na stronie internetowej pod adresem: http://www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation#4.

[57] Forgery and Counterfeiting Act 1981. Tekst dostępny na stronie internetowej pod adresem: http://www.legislation.gov.uk/ukpga/1981/45.

o podrabianiu lub przerabianiu fizycznych dokumentów. Sytuację tę na gruncie brytyjskim zmieniło wydanie w 1990 r., na wzór amerykański, szczegółowej ustawy regulującej wyłącznie kwestie przestępczości komputerowej, zatytułowanej *Computer Misuse Act*[58]. Nowa ustawa dokonała wyraźnej penalizacji czynów polegających na uzyskaniu nielegalnego dostępu do systemu oraz jego zasobów, a także dokonywaniu w nich jakichkolwiek nieuprawnionych modyfikacji, eliminując tym samym wcześniejsze trudności pojawiające się przy dokonywaniu kwalifikacji prawnych popełnionych cyberprzestępstw.

Inaczej niż w przypadku wskazanych krajów systemu *common-law*, państwa Europy kontynentalnej podejmowały głównie inicjatywy legislacyjne mające na celu uzupełnienie obowiązujących na ich terenie kodeksów karnych, zamiast wprowadzania do swoich porządków prawnych nowych aktów normatywnych o charakterze szczególnym. Rozwiązanie takie zostało przyjęte m. in. w Niemczech, Francji, czy Szwajcarii, ale także Kanadzie[59]. W tym duchu w systematyce prawa karnego umieszczane były także polskie regulacje przeznaczone do zwalczania przestępczości komputerowej, choć nie bez wyjątków stanowiących pewne koncesje na rzecz scalania przedmiotowego określonych zagadnień w odrębnych ustawach.

Na tle powyższych prac na poziomie krajowym podjęte zostały także pierwsze inicjatywy międzynarodowe mające na celu wypracowanie wspólnych standardów w tym zakresie oraz harmonizację przyjmowanych przez poszczególne kraje rozwiązań, głównie karno-materialnych. Zjawisko cyberprzestępczości zostało dostrzeżone jako problem o charakterze globalnym, wymagający przyjęcia wspólnych rozwiązań, które tak jak samo zagrożenie – również miałyby ponadnarodowy zasięg, przekraczając granice poszczególnych państw. Jako pierwsza, prace w tym obszarze podjęła Organizacja Rozwoju i Współpracy Gospodarczej (OECD), która w trakcie trwających w latach 1983 - 1986 prac grupy eksperckiej przygotowała raport zatytułowany „Przestępstwa związane z komputerem: analiza polityki legislacyjnej”[60]. Raport zidentyfikował pięć podstawowych czynów karalnych, których można dopuścić się przy pomocy technik komputerowych, a mianowicie: uzyskanie nielegalnego dostępu do systemu (dziś klasyczny *hacking*), oszustwo komputerowe, fałszerstwo komputerowe, sabotaż komputerowy oraz nielegalne powielanie programów – tzw. piractwo komputerowe.

Częściowo na skutek prac prowadzonych w ramach OECD, jeszcze w 1985 r. swoją

---

58 Computer Misuse Act. Tekst dostępny na stronie internetowej pod adresem: http://www.legislation.gov.uk/ukpga/1990/18/contents.

59 R. M. Kadir, op. cit., s. 625.

60 *Computer-related crime: Analysis of legal policy*, OECD, Paryż 1986. Cyt. za: A. Adamski, op. cit., s. 5.

działalność w zakresie analizy regulacji karnych penalizujących przestępczość komputerową, rozpoczęła kolejna grupa ekspertów, tym razem powołana jednak przez Radę Europy. Punktem wyjścia jej prac były w dużej mierze ustalenia zawarte w raporcie OECD. Efektem kilkuletnich działań grupy było wydanie przez Komitet Ministrów Rady Europy w 1989 r. Zalecenia Nr R(89)9[61] w sprawie przestępczości komputerowej. Ze względu na różnice zdań poszczególnych członków komisji w kwestii konieczności penalizacji określonych kategorii czynów, dokument podzielono na dwie części, wskazując listę czynów, które powinny być karane (tzw. lista minimalna) oraz listę tych, których karalność została pozostawiona do samodzielnej oceny przez każdy z krajów członkowskich[62]. Lista minimalna objęła łącznie osiem czynów, inkorporując „piątkę” z raportu OECD oraz dodając nowe typy przestępstw: uzyskanie nieuprawnionego dostępu do systemu, oszustwo związane z wykorzystaniem komputera, fałszerstwo komputerowe, sabotaż komputerowy, bezprawne kopiowanie programów oraz ich rozpowszechnianie oraz publikowanie, a także uszkodzenie danych lub programu, podsłuch komputerowy oraz bezprawne kopiowanie topografii półprzewodników. Lista fakultatywna wskazywała zaś na modyfikację danych lub programów, szpiegostwo komputerowe, używanie komputera bez zezwolenia oraz używanie oprogramowania komputerowego bez upoważnienia.

Implementacja postanowień Zalecenia przez kraje członkowskie nie przyniosła jednak oczekiwanych efektów z uwagi na niejednorodność wprowadzanych rozwiązań, tak w zakresie ostatecznego budowania katalogu czynów karalnych, jak i sposobu ich formułowania przez władze legislacyjne poszczególnych krajów. Wyznaczony cel harmonizacji nie został tym samym osiągnięty, częściowo obnażając nieumiejętność międzynarodowego forum państw do wspólnego budowania jednolitych rozwiązań, choć nie przekreśliło to ani wartości Zaleceń, ani zasadności samego międzynarodowego kierunku prac. Wskazane opracowanie położyło bowiem fundamenty dla wielu późniejszych dokumentów kształtujących globalne rozwiązania karne w zakresie zwalczania przestępczości komputerowej. Wybiegając nieco w przyszłość - szczególną uwagę należy zwrócić w tym miejscu na Konwencję Rady Europy o cyberprzestępczości[63], której sygnatariuszem jest także Polska. Z perspektywy czasu można stwierdzić, że dopiero kilkanaście lat starsza Konwencja stała się rzeczywistym wyrazem celów, jakie przyświecały formułowaniu Zaleceń.

---

61 *Council of Europe, Computer-Related Crime: Recommendation No. R (89)9 on computer-related crime and final report of the European Committee on Crime Problems,* Strasbourg 1989.

62 A. Adamski, op. cit., s. 7.

63 *Convention on Cybercrime CETS No.: 185*. Tekst dostępny w na stronie Internetowej pod adresem: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=03/04/2011&CL=ENG.

Po trwających cztery lata pracach Konwencja została ratyfikowana w październiku 2001 r. przez Radę Europy i pomimo pewnych głosów przeciwko (podnoszono zbyt słabą ochronę prywatności oraz praw podmiotowych), została otwarta do podpisu, oferując nie tylko zaktualizowane, ale również bardziej przemyślane rozwiązania w stosunku do dokumentów tworzonych w ramach wcześniejszych inicjatyw. Szczegółowe postanowienia Konwencji, z uwagi na swoją aktualność, zostały poddane szerszej analizie w dalszej części niniejszej pracy.

W kolejnym etapie rozwoju prawa komputerowego, który przypadł na lata dziewięćdziesiąte XX w. nastał okres umacniania ochrony prawnej własności intelektualnej oraz normatywnej implementacji idei tzw. globalnego społeczeństwa informacyjnego - zjawiska zwracającego uwagę na nie tylko ponadnarodowy, ale wręcz ponadkontynentalny zasięg wymiany informacji. Zasięg ten uzasadniał konieczność wprowadzania wspólnych regulacji o charakterze procesowym, zapewniających rzeczywistą skuteczność ścigania przestępczości popełnianej za pośrednictwem Internetu, w przypadku której sprawca działający na terenie któregokolwiek państwa ma w swoim „zasięgu" komputery ulokowane dosłownie na całym świecie. Najdonioślejszym (z punktu widzenia prawotwórstwa) przejawem wskazanej tendencji stało się wydanie w 1995 r. Zalecenia Komitetu Ministrów Rady Europy w sprawie „Problemów karnoprocesowych związanych z technologią przetwarzania informacji"[64], uzupełniającego wskazane wcześniej zalecenia z zakresu prawa karnego materialnego. Tym razem, uwaga Komitetu skupiła się na kwestiach gromadzenia dowodów, wprowadzając propozycje pewnych wspólnych rozwiązań mających na celu zaadresowanie podstawowych trudności procesowych pojawiających się w walce z przestępczością komputerową. W okresie tym, w związku z niebywała dynamiką rozwoju sieci oraz przyrostem ilości użytkowników cyberprzestrzeni, dostrzeżono także konieczność prewencyjnego ograniczania dostępności w sieci nielegalnych zasobów związanych nie tylko ze wskazanymi powyżej nadużyciami praw autorskich, ale także obejmujących znacznie szersze spektrum nielegalnych i nieakceptowanych społecznie treści związanych np. z pornografią dziecięcą.

Powyższą genealogię prawa komputerowego doskonale uzupełnia podział historii przestępczości komputerowej przedstawiony przez R. Hollingera[65], który wyróżnił w jej

[64] *Problems of Criminal Procedural Law Connected with Information Technology. Recommendation No. R (95) 13 adopted by the Committee of ministers of the Council of Europe on 11 September 1995 and explanatory memorandum, Council of Europe Publishing*, 1996.

[65] Którego efekty pracy wskazuje także sam A. Adamski, jako uzupełnienie swoich wywodów, A. Adamski, op. cit., s. 3.

ramach cztery okresy: odkrycia nadużycia komputerowego (okres od 1946 r. – powiązany z utworzeniem pierwszego publicznie znanego komputera, nazwanego ENIAC[66] - do roku 1976), okres kryminalizacji przestępczości komputerowej (lata 1977-87), okres potępienia działalności hackerskiej (1988-92, to właśnie wówczas słowo „hacker" nabrało pejoratywnego znaczenia) oraz okres cenzury (1993 do dzisiaj)[67]. Syntetycznie, opis wyróżnionych przez R. Hollingera etapów można przedstawić kolejno, jako: naukowe badania natury fenomenu przestępczości komputerowej w pierwszym okresie, poprawianie poprzez procedury legislacyjne niedostatków regulacji prawa karnego w zakresie nadużyć komputerowych w drugim, podejmowanie procesów mających na celu publiczne napiętnowanie rozszerzającej się działalności hackerskiej w trzecim oraz ograniczanie swobody dostępu do określonych kategorii informacji w czwartym[68]. Należy zauważyć, że nadejście czwartego etapu jest w dużej mierze następstwem niepowodzenia działań podjętych w okresie trzecim, w którym miały miejsce najgłośniejsze medialnie włamania komputerowe.

Analizując kolejne lata w rozwoju „komputerowego ustawodawstwa karnego", można zauważyć, że nowe przepisy przynosiły coraz to skuteczniejsze środki walki z przestępczością, umożliwiające właściwym organom podejmowanie nowych rodzajów czynności, jednak wyraźnym punktem przełomowym w tym zakresie był rok 2001. Wrześniowe ataki terrorystyczne na wieże *World Trade Center* w Nowym Jorku stały się punktem zwrotnym w historii i powodem udzielenia ogromnego publicznego mandatu do podjęcia najostrzejszych kroków w walce z terroryzmem. Wydana wówczas w USA ustawa *Patriot Act*[69] umożliwiła służbom odpowiedzialnym za bezpieczeństwo prowadzenie pełnej inwigilacji środków komunikacji elektronicznej jednocześnie ustanawiając zasadę jurysdykcyjną pozwalającą na ściganie przez Departament Sprawiedliwości USA przestępców działających przez Internet bez względu na to, gdzie faktycznie się znajdują, o ile tylko atakują komputery znajdujące się na terytorium USA[70]. Jednocześnie w USA Senat zezwolił na korzystanie z systemu *Carnivore*[71] prowadzącego w sposób automatyczny kontrolę danych przesyłanych do i z terytorium Stanów Zjednoczonych w poszukiwaniu

[66] ENIAC uważany był do roku 1975 za pierwszy komputer na świecie, jednak o miano to ubiegają się także wojskowe komputery: brytyjski Colossus oraz niemieckie maszyny Konrada Zuse. Źródło: http://pl.wikipedia.org/wiki/ENIAC.

[67] R. C. Hollinger, Crime, Deviance and the Computer, The International Library of Criminology, Criminal Justice and Penology, Aldershot: Darthmouth 1997.

[68] N. Takemura, op. cit, s. 20.

[69] Nazwa ustawy stanowi skrót od wyrazów: *Provide Appropriate Tools Required to Intercept and Obstruct Terrorism*.

[70] P. Waglowski, Prawo w sieci. Zarys Regulacji Internetu, Wydawnictwo Helion 2005, s. 296.

[71] *Ibidem*, s. 295. System Carnivore, stworzony przez FBI został ostatecznie zastąpiony innymi rozwiązaniami technicznymi, co częściowo miało na celu usunięcie pojawiających się wokół pracy systemu kontrowersji.

określonych informacji. Śladami USA poszły także kraje europejskie wprowadzając do swojego ustawodawstwa nowe środki prawne. Jako przykład wskazać należy tu między innymi ustawodawstwo brytyjskie, które dokonało odpowiednich nowelizacji ustawy RIP Act[72] regulującej kwestie kontroli komunikacji, w tym także dokonywanej za pośrednictwem Internetu. W okresie tym wiele krajów zdecydowało się także na powołanie specyficznych jednostek w strukturze organów wymiaru sprawiedliwości mających za zadanie zwalczanie przestępczości komputerowej.

Historia regulacji karnej przestępstw komputerowych na gruncie ustawodawstwa polskiego sięga września 1998 r., kiedy w życie weszły przepisy obowiązującego Kodeksu karnego[73]. Ustawa ta wprowadziła do polskiego porządku prawnego przepisy penalizujące podstawowe typy przestępstw komputerowych, jednak należy ocenić, że była w tym zakresie daleka od doskonałości. Mimo to, nowe regulacje umożliwiły dokonywanie znacznie precyzyjniejszych kwalifikacji karnych określonych czynów, które pod rządzami wcześniejszej ustawy musiałyby być przedmiotem, często bardzo trudnych, subsumcji pod normy dotyczące ogólnych, tradycyjnych form przestępczości.

Pierwsze głośne, polskie włamanie do systemu teleinformatycznego odbyło się w noc sylwestrową na przełomie roku 1995 oraz 1996, kiedy to grupa hakerów o nazwie „Gumisie" dokonała podmiany treści na internetowej stronie Naukowej i Akademickiej Sieci Komputerowej (NASK), będącej pierwszym krajowym dostawcą Internetu oraz podmiotem zarządzającym (tzw. registry) domeną .pl. Włamanie miało na celu wyrażenie niezadowolenia z podniesienia cen dostępu do sieci oraz przybrało wymiar głównie popisowy, jako, że nie wyrządziło żadnych realnych szkód poza naruszeniem dobrego imienia NASK-u - nazwa instytutu zapisana na podmienionej w wyniku ataku stronie została rozwinięta jako „Niezwykle Aktywna Siatka Kretynów"[74]. Opisywany pierwszy polski incydent komputerowy wydarzył się cztery lata po tym, gdy nawiązano pierwsze w Polsce połączenie za pośrednictwem Internetu, właśnie w NASK[75]. Jednocześnie incydent ten, stał się namacalnym dowodem, że nasze prawo karne także potrzebuje nowych, specjalistycznych środków do walki z nowoczesnymi formami przestępczości.

Obowiązujący Kodeks karny, w pierwotnym brzmieniu uchwalonym w dniu 6 czerwca 1997 r., wprowadził do polskiego porządku prawnego zaledwie kilka

---

72 *The Regulation of Investigatory Powers Act.*

73 Ustawa z dn. 6 czerwca 1997 r. - Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.).

74 Źródła:http://www.benchmark.pl/testy_i_recenzje/Internetowi_terrorysci-3063/strona/10102.html, http://www.iniejawna.pl/pomoce/haker.html.

75 Źródło: http://pl.wikipedia.org/wiki/Naukowa_i_Akademicka_Sie%C4%87_Komputerowa.

specyficznych regulacji dotyczących działań w sferze cyberprzestrzeni. Poza zasięgiem prawa pozostawiono niestety określone, liczne kategorie czynów jednoznacznie wymagające penalizacji, co wyniknęło wprost z niedostatków przyjętej redakcji. Z uwagi na historyczny charakter niniejszego rozdziału szczegółowe rozważania merytoryczne zaprezentowano w innych częściach pracy, w tym miejscu jedynie je sygnalizując.

Wprowadzone cyber-regulacje nie zostały ujęte w odrębnym rozdziale kodeksu karnego, stanowiąc w największej mierze jedynie uzupełnienie sposobu popełniania określonych przestępstw (np. art. 267 – nieuprawniony dostęp do informacji, w tym za pośrednictwem sieci) lub ich typów (np. art. 268 § 2 – niszczenie informacji, czy 278 § 2 – piractwo komputerowe). Dwa przepisy, które dotyczyły tylko i wyłącznie czynów popełnianych w cyberprzestrzeni zawarte zostały w art. 269 penalizującym tzw. sabotaż komputerowy, polegający na bezprawnej ingerencji w przetwarzanie danych o szczególnym znaczeniu dla kraju oraz w art. 287 - który wprowadził szczególną regulację oszustwa dokonywanego poprzez wpływ na przetwarzanie danych informatycznych lub ich zmianę (tzw. oszustwo komputerowe).

Dostrzegając pozytywną stronę przyjętego kierunku nowelizacji Kodeksu karnego w analizowanym zakresie, należy zauważyć, że ani przepis art. 268, ani 269 nie miały swoich odpowiedników w Kodeksie karnym z 1969 r., zaś przepis art. 267 już w oryginalnej redakcji wykazywał wiele zasadniczych zmian w stosunku do swojego odpowiednika z art. 172 § 1 dawnego Kodeksu[76]. Wprowadzenie nowych kategorii czynów niewątpliwie zapoczątkowało, trwający zresztą do dziś proces, dając podwaliny dla dalszego rozwijania regulacji karnych mających na celu zwalczanie cyberprzestępczości.

Takimi kolejnymi krokami, zarysowującymi wręcz następne etapy rozwoju krajowych regulacji prawnokarnych dotyczących zjawiska cyberprzestępczości były niewątpliwie nowelizacje Kodeksu z lat 2004[77] oraz 2008[78]. Wprowadziły one do krajowych przepisów penalizację szeregu nowych czynów, w tym także tych, które zostały błędnie pominięte w pierwotnym kształcie Kodeksu. Pierwsza nowelizacja stanowiła implementację postanowień wskazanej wcześniej Konwencji Rady Europy o cyberprzestępczości[79]. Na jej

[76] M. Kalitowski, Kodeks karny. Komentarz, Wielkie Komentarze, pod red. M. Filara, LexisNexis, Warszawa 2010, wydanie 2, s. 1144, 1145 i 1148.

[77] Ustawa z dn. 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz. U. z 2004 r. Nr 69, poz. 626).

[78] Ustawa z dn. 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. z 2008 r. Nr 214, poz. 1344).

[79] *Convention on Cybercrime CETS No.: 185*. Tekst dostępny na stronie Internetowej pod adresem: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=03/04/2011&CL=ENG.

mocy dodane zostały do Kodeksu karnego przepisy art. 268a (niszczenie danych informatycznych), 269a (zakłócenie pracy systemu, w tym co bardzo istotne - ataki typu *dos* oraz *ddos*) oraz 269b (penalizujący określone przejawy działalności hackerskiej, crackerskiej, ale także *phishing*). Znowelizowane zostały ponadto m.in. przepisy art. 287 § 1 (oszustwo komputerowe) oraz 130 § 3 (szpiegostwo).

Druga ze wskazanych wyżej nowelizacji miała na celu dostosowanie polskiej ustawy karnej do postanowień Decyzji ramowej Rady z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[80]. Ustawa nowelizująca z 2008 r. przede wszystkim zmieniła brzmienie art. 267, który od jej wejścia w życie objął swoim zakresem przedmiotowym już samo uzyskanie dostępu do informacji, podczas gdy do tej pory karane było dopiero bezpośrednie uzyskanie tejże informacji[81]. Nowe brzmienie nadano także art. 269a, który objął utrudnienie dostępu do danych, sankcjonując ataki typu *dos* oraz *ddos* (odmowa dostępu oraz rozproszona odmowa dostępu).

Obok regulacji karnych, polski porządek prawny został uzupełniony także o szereg innych przepisów z zakresu prawa cywilnego oraz administracyjnego. Wprowadzenie podpisu elektronicznego, możliwości zawierania umów na odległość, świadczenia usług drogą elektroniczną, tzw. e-bankowości, elektronicznych Biuletynów Informacji Publicznej, czy wreszcie samej informatyzacji działalności podmiotów realizujących zadania publiczne - każdorazowo wiązały się ze zmianami prawa. W tym miejscu szczególną uwagę należy zwrócić jednak na dwa akty normatywne – ustawę o podpisie elektronicznym z 2001 r.[82], penalizującą między innymi bezprawne posługiwanie się tym rodzajem podpisu oraz ustawę o świadczeniu usług drogą elektroniczną z 2002 r.[83], implementującą postanowienia europejskiej dyrektywy z 2000 roku[84].

Tematyka procesów informatyzacji kraju, jak również stosowania prawa karnego w obszarze cyberprzestępczości, przedziera się na przestrzeni ostatnich lat także do doktryny prawniczej orientującej się na wymiar praktyczny zwalczania tej gałęzi przestępczości. Istotnym przykładem jest tutaj przede wszystkim cykl konferencji naukowych

---

[80] Decyzja ramowa Rady Nr 2005/222/WSiSW z 24 lutego 2005 r. w sprawie ataków na systemy informatyczne.

[81] B. Kunicka-Michalska, Duże Komentarze Becka Tom II, pod red. prof. A. Wąska i prof. R. Zawłockiego, s. 685 i nast.

[82] Ustawa z dn. 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.)

[83] Ustawa z dn. 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1244, z późn. zm.)

[84] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego, w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym).

organizowanych pod auspicjami Wyższej Szkoły Policji, pn. „Przestępczość teleinformatyczna”[85]. Odrębnie, należy także zaznaczyć inicjatywy podejmowane przez środowiska komercyjne, reprezentowane przez firmy świadczące usługi z obszaru bezpieczeństwa teleinformatycznego, które zmierzają do ujęcia prowadzonej działalności w możliwie precyzyjne ramy prawne[86]. Jako swoisty przykład aktywności polskich prawników na arenie międzynarodowej w obszarze analizowania zagadnień związanych z owoczesnymi formami przestępczości można także wskazać na udział polskiej delegacji rządowej (w składzie m.in. prof. E. Pływaczewski oraz prof. W. Filipkowski) w XII Kongresie Organizacji Narodów Zjednoczonych, który to Kongres odbył się w Salwadorze, w dniach 12-19 kwietnia 2010 r.[87]. W czasie Kongresu polska prezentacja dorobku naukowego wypracowanego w ramach realizowanych projektów naukowo-badawczych dot. m.in. wykorzystania nowoczesnych technologii przez sprawców przestępstw, spotkała się z najwyższą oceną ze strony uczestników Kongresu.

PODSUMOWANIE

Powyższe ujęcie historyczne zakończyć należy następującym podsumowaniem:

- wraz z pojawieniem się nowych (*cybernetycznych*) rodzajów aktywności ludzkiej - realizowanych pierwotnie w rozległych sieciach telekomunikacyjnych oraz później w cyberprzestrzeni, wykształciły się nowe formy przestępczości. Ich *novum* było opieranie *modus operandi* sprawcy na możliwości wykorzystania technicznych słabości systemów teleinformatycznych oraz braku odpowiedniej wiedzy po stronie użytkowników,
- choć prawdziwy rozwój cyberprzestępczości należy datować na lata osiemdziesiąte ubiegłego stulecia, pierwsze przejawy przestępczości komputerowej opisywane były w prasie amerykańskiej jeszcze dwadzieścia lat wcześniej, to jest w latach

[85] Przykładowe materiały poseminaryjne: J. Kosiński J. (pod red.), Przestępczość teleinformatyczna: IX seminarium naukowe: materiały seminaryjne, WSPol, Szczytno 2006; J. Kosiński (pod red.), Przestępczość teleinformatyczna: X seminarium naukowe: materiały poseminaryjne, WSPol, Szczytno 2007; J. Kosiński (pod red.), Szafrański J. (pod red.), Przestępczość teleinformatyczna: XI seminarium naukowe: materiały poseminaryjne, WSPol, Szczytno 2008.

[86] Jako przykład można wskazać na opracowanie zbiorowe: S. Małycha (wstęp), Informatyka śledcza okiem prawników, materiały Mediarecovery, Media Sp. z o.o., Warszawa 2014, opracowanie dostępne na stronie internetowej pod adresem: https://magazyn.mediarecovery.pl/wp-content/uploads/prawnicy.pdf.

[87] Więcej na temat konferencji: E. W. Pływaczewski, Zapobieganie przestępczości i sprawiedliwość karna. XII Kongres Organizacji Narodów Zjednoczonych (Salwador, Brazylia, 12-19 IV 2010), Państwo i Prawo 2010, z. 10, s. 133 i nast.

sześćdziesiątych. W istocie, przestępczość komputerowa jest omal w równym wieku z zastosowaniem komputerów,

- pierwsze zmiany prawa karnego nakierowane na zwalczanie przestępczości komputerowej zaczęły obowiązywać w ustawodawstwie USA pod koniec lat siedemdziesiątych. Rozkwit tego rodzaju prawodawstwa w Europie przypada na przełom lat osiemdziesiątych i dziewięćdziesiątych (na początku Włochy, później - Wielka Brytania, Dania, RFN, Szwecja, Austria, Norwegia, Francja, NRD oraz Grecja,
- powstała w ramach zaznaczonego powyżej procesu legislacyjnego gałąź prawa, zwana często prawem komputerowym, pozwala na uznanie swoistego usankcjonowania cyberprzestrzeni, jako kategorii prawnej, posiadającej określone regulacje szczególne oraz specyficzny kontekst interpretacyjny. Można stwierdzić, iż aktualnie wszystkie państwa rozwinięte, w których funkcjonują społeczeństwa informacyjne, posługują się szeregiem aktów normatywnych regulujących liczne aspekty funkcjonowania cyberprzestrzeni: wykorzystywania jej zasobów, posługiwania się podpisem elektronicznym, świadczenia usług drogą elektroniczną, świadczenia e-usług przez podmioty publiczne, czy wreszcie zwalczania nowoczesnych zagrożeń oraz przestępstw cybernetycznych,
- wyrażając szczególną przeciwwagę do powyższych tez – cyberprzestrzeń, jako obszar pozbawiony granic, niepoddający się prostemu podziałowi pomiędzy jurysdykcje poszczególnych państw oraz *de facto* bezpaństwowy (cyberprzestrzeń, jako domena logiczna nie zaś zbiór zasobów, nie należy do nikogo) – wymyka się jednak tradycyjnemu pojmowaniu instytucji prawnych, wskazując istotne odmienności w stosunku do sposobu regulowania działań ludzkich w otaczającej nas rzeczywistości fizycznej (choćby kwestia automatyzacji działań podejmowanych w cyberprzestrzeni niezwykle utrudniająca wyznaczenie granic prywatności jej użytkowników). Odmienności te stanowią jeden z głównych przedmiotów badań w niniejszej pracy,
- z uwagi na ponadkrajowy charakter cyberprzestrzeni – oraz w konsekwencji analogicznie światowy charakter występujących w niej zagrożeń, obok regulacji krajowych, analizowany obszar stał się także przedmiotem licznych przepisów o charakterze międzynarodowym, powstających zarówno w ramach prawodawstwa Unii Europejskiej (jak np. Decyzja Ramowa Rady Unii Europejskiej w sprawie ataków na systemy informatyczne oraz zastępująca ją Dyrektywa Parlamentu

Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne), jak również szczególnych inicjatyw międzynarodowych, nakierowanych specyficznie na zwalczanie nowych zagrożeń cybernetycznych (w szczególności wskazać należy tu na budapesztańską Konwencję o cyberprzestępczości z 2001 r.).

Powyższe podsumowanie – skupiające się *de facto* na pojawieniu się nowego obszaru cyfrowej rzeczywistości oraz wykształceniu w jego środowisku nieznanych wcześniej form przestępczości, pozwala na płynne przejście do części merytorycznej pracy, która zaczyna się od próby określenia, czym na gruncie aktualnie obowiązujących regulacji prawnych oraz aktów około-prawnych jest *cyberprzestrzeń* oraz *cyberprzestępczość*.

Rozdział II
Cyberprzestrzeń oraz przestępczość w cyberprzestrzeni - zagadnienia definicyjne

§ 1. Definiowanie cyberprzestrzeni

Za punkt wyjścia dla prowadzenia dalszych rozważań merytorycznych na temat specyfiki przestępstw popełnianych w cyberprzestrzeni należy uznać próbę określenia, czym (oraz gdzie?) jest (znajduje się?) sama cyberprzestrzeń. Pomimo bowiem, iż na gruncie obowiązującego w Polsce Kodeksu karnego, obszar ten nie funkcjonuje jako legalnie wyodrębniona, szczególna przestrzeń dla popełniania czynów zabronionych, specyfika cyberprzestrzeni (pozbawiona fizycznych wymiarów, czy też możliwości typowej, geograficznej atrybucji działań człowieka) niejako warunkuje specyfikę całej gałęzi przestępczości komputerowej. *De facto* bowiem, to właśnie pojawienie się tej nowej cyfrowej domeny wykreowało szeroki katalog nieznanych dotąd czynów bezprawnych, których powagi nikt już dzisiaj nie neguje. Do najbardziej znanych przestępstw powstałych dzięki pojawieniu się cyberprzestrzeni zaliczyć można hacking, organizowanie ataków mających na celu przerwanie świadczenia określonych usług (tzw. ataki *Dos* oraz *Ddos* – odmowy dostępu), szpiegowanie w sieci, czy stosowanie nowoczesnych metod inżynierii społecznej umożliwiających podszywanie się pod podmioty prowadzące określone rodzaje działalności za pośrednictwem Internetu.

Ponieważ cyberprzestrzeń stanowi obszar wytworzony w oparciu o nowoczesne technologie informatyczne, jej definiowanie jest w istocie zadaniem interdyscyplinarnym. Odnośne rozważania prawnicze dotykają tu podstaw technicznych budowy cyberprzestrzeni, których poznanie jest kluczowe dla zrozumienia specyfiki zjawiska cyberprzestępczości. Jednocześnie, cyberprzestrzeń tworząc nowe rodzaje zachowań oraz powiązań społecznych stanowi zarazem istotny obszar badań o charakterze socjologicznym. Cyberprzestrzeń bowiem, w ujęciu funkcjonalnym, tworzona jest najogólniej przez: a) technologiczną infrastrukturę umożliwiającą jej funkcjonowanie, w tym zachodzenie procesów wymiany danych oraz informacji (m. in. wszystkie elementy tworzące sieci komputerowe oraz sieci telekomunikacyjne – komputery, serwery, centrale, łącza, wraz z oprogramowaniem wyposażonym w interfejsy użytkownika); b) specyficzne reguły, zarówno prawne, jak i te

niesformalizowane, rządzące zachowaniami w jej obszarze; oraz c) działania użytkowników poruszających się po jej zasobach oraz podejmujących wzajemne interakcje. W uproszczeniu zatem, uznać należy, że cyberprzestrzeń jest obszarem społecznego doświadczenia podejmowanego za pośrednictwem technologii informatycznych – głównie komputerów z zainstalowanym oprogramowaniem, gdzie jednostki, z pominięciem geograficznych granic oraz wymiarów, mogą wzajemnie oddziaływać na siebie wywołując także określone (jak najbardziej rzeczywiste) skutki prawne[88]. Przedstawioną definicję można dodatkowo uzupełnić o zautomatyzowane relacje samych komputerów oraz innych maszyn (w tym w szczególności urządzeń typu *smart glass*, elementów tzw. inteligentnych domów, czy też nowoczesnych systemów energetycznych oraz pomiarowych - by wymienić tylko kilka przykładów), wpisujące się w zdobywającą c popularność ideę Internetu Rzeczy (z ang. *Internet of Things*). Wedle przywołanej koncepcji inteligentne maszyny, łącząc się poprzez globalną sieć, zyskują atrybuty swoistych kolonii zdolnych nie tylko do komunikacji, ale także prymitywnej samoorganizacji i optymalizacji[89].

Chociaż wyrażenie *cyberprzestrzeń* wciąż uważane jest za bardzo nowoczesne, jego historia sięga dziś już przeszło dwudziestu lat[90]. Po raz pierwszy pojęciem tym posłużył się William Gibson[91] - uznany autor powieści *science-fiction*, który zaproponował to określenie w swojej krótkiej noweli zatytułowanej *Burning Chrome*[92] oraz później spopularyzował w powieści *Neuromancer*[93]. W. Gibson zdefiniował cyberprzestrzeń (w oryginale *cyberspace*) w tej drugiej pozycji jako:

> „Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych… Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność... Świetlne linie przebiegały bezprzestrzeń umysłu, skupiska i konstelacje danych.”[94]

---

88 Definicja złożona z wybranych elementów, na które wskazują w swoich licznych opracowaniach m. in. N. Takemura, A. Suchorzewska, M. Castells, R. Ottis, P. Lorents, R. Geist, D. R. Johnson, D. G. Post oraz niezliczone źródła internetowe.

89 Więcej na temat koncepcji Internetu Rzeczy: M. Kołodziej, Internet Rzeczy, nowe spojrzenie na ochronę prywatności, s. 12 i nast., w: J. Kosiński, Przestępczość teleinformatyczna 2015, Szczytno 2015.

90 L. Duff, S. Gardiner, *Compuer Crime in the Global Village: Strategies for Control and Regulation – in Defence of the Hacker*, w: D. S. Wall, *Cyberspace Crime*, Wyd. Ashgate, Anglia 2003, s. 145.

91 Tak w: http://www.thecybernaut.org/2010/11/definitions-of-cyberspace/,czy http://en.wikipedia.org/wiki/Cyberspace

92 Nowela została opublikowana w 1982 r. w magazynie *Omni*, amerykańskim piśmie poświęconym tematyce *science-fiction*.

93 W. Gibson, Neuromancer, Ace Books, Nowy York 1984.

94 Fragment książki w tłumaczeniu Piotra W. Cholewy, Wydawnictwo Książnica, Katowice 2009, s. 59. W oryginale: *“A consensual hallucination experienced daily by billions of legitimate operators, in every*

Przytoczona definicja, chociaż pochodząca z powieści beletrystycznej, nie tylko dała podwaliny do późniejszych naukowych rozważań nad istotą cyberprzestrzeni, ale wskazała także jej podstawowe elementy: rozległość (zasięg światowy), spajanie wszelkich zasobów w jedną, olbrzymią bazę danych, złożoność oraz *bez-przestrzenność* rozumianą jako brak możliwości odniesienia cyberprzestrzeni do wymiarów fizycznych *realnego* świata. Definicja wprowadzała jednocześnie wizualizację cyberprzestrzeni („graficzne odwzorowanie"), co stało się elementem charakterystycznym dla ówczesnej fantastyki określanej mianem *cyberpunku*[95].

Jako jedne z najgłośniejszych przykładów prac reprezentujących ten nurt współczesnej kultury należy wskazać trylogię filmów *Matrix*[96], czy nieco wcześniejszą produkcję *Johnny Mnemonic*[97]. Choć nieosadzony ściśle w tym gatunku, wizję postrzegalnej zmysłami cyberprzestrzeni prezentował także *Tron: Dziedzictwo*[98], będący kontynuacją głośnego filmu z lat osiemdziesiątych XX wieku. Zawarta w wymienionych tytułach wizja cyberprzestrzeni przedstawiała ją w formie przestrzeni zobrazowanej przy wykorzystaniu grafiki komputerowej – funkcjonującej niczym obraz w grze komputerowej, pełen trójwymiarowych, interaktywnych obiektów poruszających się we wspólnym środowisku z zachowaniem perspektywy oraz znanych nam z rzeczywistości zjawisk fizycznych, jak grawitacja, czy kolizja obiektów. Wizualizacja ta pozwalała przypisywać cyberprzestrzeni cechy właściwe realnej, postrzegalnej zmysłami rzeczywistości, którą można nie tylko zobaczyć, ale również dotknąć i kształtować. Zagadnienie to stało się jednym z elementów pojęcia wirtualnej rzeczywistości[99], oznaczającego nieistniejącą fizycznie, lecz logicznie, przestrzeń, którą dla

---

nation, by children being taught mathematical concepts… A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data.". Tekst angielski przytaczam za stroną internetową pod adresem: http://www.thecybernaut.org/2010/11/definitions-of-cyberspace/.

95 Wyrażenie powstało na początku lat '80. Jego twórcą jest powieściopisarz Bruce Bethke, autor książki zatytułowanej właśnie „Cyberpunk". Najbardziej charakterystycznymi cechami gatunku jest przedstawianie wizji przyszłości, w której ludzie, komputery oraz maszyny a także ich środowiska zaczynają się wzajemnie przenikać.

96 Na trylogię składają się: Matrix (1999 r.), Matrix: Reatkywacja (2003 r.) oraz Matrix: Rewolucje (również 2003 r.). Za stworzenie scenariusza filmu odpowiedzialni byli bracia o polskich korzeniach, Andy oraz Larry Wachowscy.

97 Premiera filmu odbyła się w 1995 r. Jego fabuła była luźno powiązana w powieścią pod tym samym tytułem autorstwa W. Gibsona.

98 Tron: Dziedzictwo, będący kontynuacją filmu Tron, został wydany w 2011 r. Część pierwsza ukazała się natomiast w roku 1982. W obu produkcjach przedstawiono wizję cyberprzestrzeni jako cyfrowego świata, zbudowanego na siatce przypominającej kratki w zeszycie. W przedstawionej wirtualnej rzeczywistości wszystko przybierało postać zobrazowaną – np. programy chroniące system miały kształt futurystycznych maszyn, inspirowanych kształtem czołgów, zbudowanych z czarnych bloków. Pierwsza część filmu stała się swojego rodzaju hymnem pasjonatów nowoczesnych technologii.

99 Pojęcie, w nowoczesnym rozumieniu, pochodzi z języka angielskiego, gdzie w oryginale brzmi *virtual reality*. Za jego autorów oraz jednocześnie popularyzatorów uważa się Howarda Rheingolda oraz Michaela

ułatwienia jej uchwycenia, można wyobrażać sobie właśnie w postaci zobrazowanej oraz rozumianej trójwymiarowo. Nie oznacza to jednocześnie, że przestrzeń ta musi być pełnym odbiciem naszej fizycznej rzeczywistości, gdyż chodzi tu o samą ideę wyobrażenia swojego rodzaju równoległego, nieistniejącego fizycznie świata, nazywanego w oryginalnej definicji cyberprzestrzeni „konsensualną halucynacją". Stosunek pojęciowy zachodzący pomiędzy cyberprzestrzenią a wirtualną rzeczywistością jest zatem taki, że o ile cyberprzestrzeń odnosi się, w uproszczeniu, do obszaru szeroko rozumianego przetwarzania danych przez systemy teleinformatyczne, o tyle wirtualizacja rzeczywistości polega na konceptualnym kreowaniu nie-fizycznego świata oraz nadawaniu jego przestrzeni (niektórych) cech realności, właściwych otaczającej nas rzeczywistości.

Istotnym dla pełnego zrozumienia pochodzenia terminu *cyberprzestrzeń* jest także przybliżenie innego wyrażenia, które stało się niejako inspiracją dla W. Gibsona. Terminem, który zapoczątkował budowanie słów poprzedzonych przedrostkiem *cyber*- była *cybernetyka* (*cybernetics*) przedstawiona przez Norberta Weinera jeszcze w 1948 r. N. Weiner zdefiniował to pochodzące z greki wyrażenie[100], jako „kontrolę oraz komunikację pomiędzy światem zwierząt oraz maszyn"[101]. To właśnie przedstawiona przez Weinera koncepcja nowych form interakcji pomiędzy ludźmi oraz maszynami, które to interakcje tworzą w istocie nowy system funkcjonujący w nieznanym dotąd środowisku, stała się punktem wyjścia dla stworzenia pojęcia cyberprzestrzeni[102]. Powstała era, w której świat maszyn i zwierząt wzajemnie się przeniknął.

1. Regulacje w wybranych państwach na świecie

Z uwagi na rosnące znaczenie systemów teleinformatycznych wykorzystywanych dziś przez społeczeństwa na całym świecie, w tym też tworzących elementy państwowej infrastruktury krytycznej niezbędnej dla poprawnego realizowania zadań na rzecz obywateli, współczesna doktryna prawna również zaczęła się interesować definiowaniem cyberprzestrzeni. Ilość specyficznych działań podejmowanych przez ludzi za pośrednictwem

---

R. Heima, którzy posługiwali się omawianym pojęciem w latach '90. Sama koncepcja datuje się jednak na okres wcześniejszy, przypadający na lata siedemdziesiąte. Zaznaczyć należy także, że samo pojęcie *wirtualny* oznacz tyle co „mogący zaistnieć". Więcej o zastosowaniu pojęcia wirtualnej rzeczywistości na internetowej stronie pod adresem: http://en.wikipedia.org/wiki/Virtual_reality#cite_note-2.

[100] Z greki *kybernetes* – sternik, zarządca. Za internetową encyklopedią PWN: http://encyklopedia.pwn.pl/haslo.php?id=3888555.

[101] N. Wiener, Cybernetics: Or Control and Communication in the Animal and the Machine, John Wiley & Sons, New York 1948. Przytoczona definicja zawarta jest w samym tytule pracy.

[102] R. Ottis, P. Lorents, *Cyberspace: Definition and Implications*, s. 1. Praca napisana w ramach publikacji tworzonych przez centrum *Cooperative Cyber Defence Centre of Excellence* ulokowane w Tallinie. Opracowanie dostępne na stronie internetowej CCDCOE pod adresem: http://www.ccdcoe.org/205.html.

komputerów oraz sieci (tak komputerowych, jak i telefonicznych) spowodowała bowiem konieczność rozpoznania nowego cyfrowego środowiska, które nadało zupełnie nowy kształt zawieraniu umów cywilnoprawnych, dokonywaniu czynności administracyjnych, ale także popełnianiu nowoczesnych form przestępczości – oraz w reakcji, działaniom podejmowanym w celu zapobiegania oraz wykrywania tego typu zachowań.

Przechodząc do bliższej analizy specyficznych cech cyberprzestrzeni, należy przyjrzeć się kilku współczesnym, prawniczym definicjom tego pojęcia. Podkreślenia wymaga jednak w tym miejscu fakt, że żadna z przedstawianych definicji nie została zawarta w dokumencie stanowiącym powszechnie obowiązujące źródło prawa karnego, które byłoby odpowiednikiem naszej ustawy.

Jedna z szeroko rozpoznawanych jako punkt wyjściowy oraz powszechnie cytowanych dziś definicji cyberprzestrzeni została sformułowana w ramach prac amerykańskiego Departamentu Obrony (*US Department of Defense,* odpowiednik Ministerstwa Obrony Narodowej) mających na celu stworzenie jednolitego słownika terminologii wojskowej oraz powiązanej. Słownik ten nazywany jest w skrócie JP 1-02[103]. W zawartej w nim definicji możemy przeczytać, że cyberprzestrzeń to:

> „Globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT), włączając Internet, sieci telekomunikacyjne, systemy komputerowe a także osadzone w nich procesory oraz kontrolery."[104]

Charakterystyczną cechą przytoczonej definicji jest brak odwoływania się w niej do jakichkolwiek elementów społecznych, czy w ogóle do ludzi będących użytkownikami cyberprzestrzeni – podczas, gdy składniki te były istotną częścią oryginalnego rozumienia pojęcia cyberprzestrzeni. Przedstawiona definicja Departamentu Obrony skupia za to całą swą uwagę na technologicznym aspekcie fundamentów cyberprzestrzeni. Jak słusznie jednak podnosi się w literaturze przedmiotu[105], ów aspekt technologiczny został poruszony w definicji wprost jedynie w ograniczonym zakresie przedmiotowym: definicja *expressis verbis* wskazuje jedynie na sprzętową stronę infrastruktury tworzącej cyberprzestrzeń, pomija zaś jej warstwę programową, której istnienie na gruncie definicji musi być domniemywane.

[103] *Joint Publication 1-02, Department of Defense, Dictionary of Military and Associated Terms*. Wersja z 15 maja 2011 r. Dokument dostępny jest na stronie internetowej Technicznego Centrum Informacji nt. Obrony, pod adresem: http://www.dtic.mil/doctrine/dod_dictionary.

[104] *Joint Publication 1-02*, s. 93. W oryginale: "*A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*.". Tłumaczenie własne.

[105] R. Ottis, P. Lorents, op. cit., s. 2.

Oceniając omawiany zabieg autorów definicji należy mieć jednak na uwadze jej wojskowe pochodzenie oraz zastosowanie. Dzięki przedstawionemu uproszczeniu, definicja w zamian doskonale odzwierciedla dwie inne istotne cechy cyberprzestrzeni: pierwszą, wskazującą, że cyberprzestrzeń stanowi potencjalny teatr działań obejmujący zasięgiem całą kulę ziemską (*globalna domena*) oraz drugą, charakteryzującą rozległe powiązania infrastrukturalne łączące sieci różnych rodzajów, w tym - co istotne - zarówno prywatne, jak i stanowiące własność państwową. Na marginesie, warto w tym miejscu także zaznaczyć, że zaprezentowana definicja wyraźnie inkorporuje do swojego zakresu globalną sieć Internet – wymienioną tu wprost z nazwy. Z punktu widzenia doktryny wojskowej, wskazane wyżej cechy cyberprzestrzeni odnoszą się odpowiednio do możliwości podjęcia w ramach cyberprzestrzeni działań militarnych oraz do określenia fizycznych składników sieci, które podlegać muszą szczególnej ochronie. Wynikiem przyjęcia tej koncepcji jest zawarta także w słowniku JP 1-02 definicja pojęcia „operacji w cyberprzestrzeni", określająca działania te jako „zastosowanie *cyber-możliwości (działań)* w przypadkach, gdzie głównym celem jest osiągnięcie zamierzeń w cyberprzestrzeni lub za jej pośrednictwem. W zakres takich operacji wchodzą operacje w sieciach komputerowych oraz działania mające na celu wykorzystanie oraz ochronę Globalnej Sieci Informacyjnej."[106]. Globalną Siecią Informacyjną nazywane są zaś systemy wykorzystywane przez armię do realizacji jej zadań, w tym krajowe systemy bezpieczeństwa.

Definiując cyberprzestrzeń jako domenę działań warto także w tym miejscu zwrócić uwagę na pewną szczególną cechę tej domeny - choć oczywistą, to jednak osobliwą i często pomijaną w rozważaniach. Cyberprzestrzeń stanowiąc wytwór ludzki, nie posiada bowiem naturalnych, „wrodzonych" cech, jakie charakteryzują sfery lądu, powietrza, czy wody, będące teatrem dla konwencjonalnych działań militarnych. Tym samym, wyjaśnienie specyfiki cyberprzestrzeni nie może odnosić się do kwantyfikatorów opisujących realne wymiary, jak długość, czy szerokość. Cyberprzestrzeń, choć oparta na elementach infrastrukturalnych rozrzuconych dosłownie po całym świecie (co także implikuje jej ponadnarodowość), w ujęciu teoretycznym stanowi bowiem domenę logicznie oderwaną (*suwerenną*) od swojej fizycznej podbudowy[107]. Cyberprzestrzeń zatem to nie same systemy teleinformatyczne, ale obszar przetwarzania danych, który dzięki nim istnieje. Błędem jest zatem wyrażone w definicji utożsamianie sieci oraz wchodzących w ich skład komputerów

---

[106] *Joint Publication 1-02*, s. 93. W oryginale: "*The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.*".

[107] *Cyberspace Operations, Air Force Doctrine Document 3-12*, wersja z 15. lipca 2010 r.

z cyberprzestrzenią, tak jak zbyt daleko idącym skrótem myślowym zastosowanym w analizowanym dokumencie wojskowym – powodującym w istocie błąd o charakterze jakościowym, jest automatyczne ustawianie cyberprzestrzeni na jednej linii z pozostałymi obszarami działań wojskowych – wspomnianymi lądem, powietrzem oraz wodą. Cyberprzestrzeń nie posiadając bowiem cech właściwych sferom fizycznym, nie kwalifikuje się do wyodrębniania przy zastosowaniu wspólnego kryterium podziału - brak tu cechy, która pozwoliłaby oddzielić cyberprzestrzeń np. od powietrza w sposób analogiczny jak oddziela się np. wodę od lądu. Zabieg ten, należy jednak ocenić, zastosowany został jako praktyczne uproszczenie siatki terminologicznej, choć wymagające opatrzenia stosownym komentarzem dla poprawnego zrozumienia prezentowanej problematyki.

Wybierając kolejną definicję cyberprzestrzeni do bliższej analizy, warto sięgnąć po jeszcze jedną oficjalną propozycję pochodzącą z doktryny amerykańskiej, stworzoną jednak dla potrzeb realizacji zadań nałożonych na administrację cywilną tego państwa. Zestawienie tej definicji z wcześniej zaprezentowaną pozwoli bowiem porównać rozkład akcentów, jaki różni spojrzenia wojskowe oraz cywilne.

W przyjętej w 2003 r. przez Biały Dom Narodowej Strategii dla Bezpiecznej Cyberprzestrzeni[108] zapisano wpierw we wstępie krótką, wprowadzającą definicję cyberprzestrzeni, określającą ją jako *współzależną sieci infrastruktury technologii informacyjnej*, by w dalszej części opracowania zamieścić znacznie bardziej rozbudowany opis tego pojęcia, przedstawiony poniżej:

> „Nasza Krajowa infrastruktura krytyczna budowana jest przez publiczne, jak i prywatne instytucje funkcjonujące w sektorach rolnym, żywieniowym, zaopatrzenia w wodę, służby zdrowia, usług ratunkowych, rządowym, obronnym, przemysłowym, informacyjnym oraz telekomunikacyjnym, energetycznym, transportowym, bankowym oraz finansowym, chemicznym oraz materiałów niebezpiecznych a także pocztowym oraz dostawczym. Cyberprzestrzeń stanowi ich układ nerwowy – system kontrolny naszego kraju. Cyberprzestrzeń zbudowana jest z setek tysięcy połączonych komputerów, serwerów, routerów, switchy oraz światłowodów, które umożliwiają pracę naszej infrastrukturze krytycznej. Stąd też, zdrowe funkcjonowanie cyberprzestrzeni jest

[108] Narodowa Strategia dla Bezpiecznej Cyberprzestrzeni, tytuł oryginalny: *National Strategy to Secure Cyberspace*. Dokument został sporządzony jako jeden z elementów odpowiedzi na zamach terrorystyczny z 11 września 2001 r. Treść strategii została opracowana przez Departament Bezpieczeństwa Krajowego (*Department of Homeland Security*) oraz zatwierdzona w kwietniu 2003 r. Tekst strategii dostępny na stronie internetowej pod adresem: http://www.dhs.gov/files/publications/editorial_0329.shtm.

kluczowe dla naszej ekonomii oraz bezpieczeństwa narodowego."[109]

Uzupełniająco, należy także wskazać, że *Strategia* w swojej dalszej treści określa, że *amerykańska cyberprzestrzeń* łączy Stany Zjednoczone z resztą świata[110] poprzez sieci o globalnym zasięgu, a także posługuje się dodatkowymi pojęciami Cyberprzestrzeni Krajowej (*National Cyberspace*) oraz Cyberprzestrzeni Rządowej (*Governments Cyberspace*) choć bez bliższego wyjaśniania ich treści.

Zawarta w strategii bezpieczeństwa szeroka definicja cyberprzestrzeni wskazuje nie tylko na liczność oraz rozległość elementów infrastrukturalnych wraz z ich powiązaniami z krajową infrastrukturą krytyczną, której poprawne funkcjonowanie stanowi fundament dla realizacji zadań państwa, ale także na aspekt społeczno-ekonomiczny funkcjonowania cyberprzestrzeni. Nazywanie cyberprzestrzeni układem nerwowym wszelkich sektorów gospodarczych oraz administracyjnych stanowi jednoznaczny wyraz wagi, jaką przywiązuje się w Stanach Zjednoczonych do zagadnień krajowej informatyzacji oraz roli tego procesu w budowaniu nowoczesnego państwa[111]. To właśnie cyberprzestrzeń, stanowiąca nowoczesny, w dużej mierze zautomatyzowany obszar natychmiastowej wymiany ogromnych ilości informacji, prezentowana jest w przytoczonej definicji jako główny ośrodek krajowej działalności gospodarczej. W istocie, niefunkcjonowanie dziś w np. w Internecie, będącym jak wskazują definicje jednym z podstawowych elementów cyberprzestrzeni, oznacza w wysoko rozwiniętych krajach poważne ograniczenie udziału w nowoczesnej wymianie rynkowej. Należy zaznaczyć, że definicja nie wskazując wprost na udział ludzi w cyberprzestrzeni, czyni to jednak pośrednio odwołując się do funkcjonowania szeroko rozumianej gospodarki krajowej.

Istotna dla zrozumienia wizji cyberprzestrzeni przedstawionej w Narodowej Strategii dla Bezpiecznej Cyberprzestrzeni jest także próba przybliżenia treści przywołanych wcześniej pojęć cyberprzestrzeni krajowej oraz rządowej. Analizowany dokument wprowadza, niestety

---

[109] Narodowa Strategia dla Bezpiecznej Cyberprzestrzeni, *Executive Summary*, s. vii. W oryginale: „*Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public, health, emergency services, government, defense, industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security*.". Tłumaczenie własne.

[110] Narodowa Strategia dla Bezpiecznej Cyberprzestrzeni, s. xii.

[111] Dla przykładu, w konferencji, która odbyła się w dniu 29 maja 2009 r. poświęconej kwestii bezpieczeństwa w cyberprzestrzeni Prezydent Stanów Zjednoczonych Barack Obama oświadczył, że "Cyberzagrożenia stanowią jedno z największych wyzwań dla bezpieczeństwa ekonomicznego i krajowego, przed którym stajemy jako naród." oraz, że „Powodzenie amerykańskiej ekonomii w dwudziestym pierwszym wieku zależeć będzie od poziomu cyberbezpieczeństwa". Nagranie z konferencji dostępne jest na stronie internetowej Białego Domu pod adresem: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity.

bez bliższego opisu, koncepcję wydzielenia amerykańskiej cyberprzestrzeni, jak należy domniemywać, z cyberprzestrzeni światowej, bądź też z cyberprzestrzeni pozostałych państw. Rozdzielenie to należy prawdopodobnie rozumieć, jako próbę wyznaczenia obszaru pozostającego pod bezpośrednią jurysdykcją Stanów Zjednoczonych. Idea ta w praktyce pozostaje jednak zupełnie nieefektywna z uwagi na specyficzne cechy cyberprzestrzeni, która, jak wskazano przy prezentacji definicji zawartej w słowniku JP 1-02, stanowiąc obszar logiczny, odrywa się od infrastruktury stanowiącej jej fizyczny substrat oraz kryteriów geograficznych. Skuteczne wyodrębnienie cyberprzestrzeni jednego państwa mogłoby odbyć się jedynie przy założeniu pełnej separacji infrastruktury tworzącej taką krajową cyberprzestrzeń, pozostającą pod wyłączną władzą jednego kraju.

Przechodząc na grunt europejski – wbrew pozorom bogaty w przedmiotowym zakresie, analizę badanego pojęcia „cyberprzestrzeń" należy zacząć od przybliżenia definicji przedstawionej na szczeblu Unii Europejskiej. W oficjalnym elektronicznym słowniku pojęć z zakresu społeczeństwa informacyjnego, możemy zapoznać się z zaproponowaną przez Komisję Europejską definicję cyberprzestrzeni, określającą ją jako:

> „Wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata."[112]

Elementem podstawowym jest tu *przestrzeń wirtualna*, pojęcie z którego uczyniono *genus* prezentowanej definicji. Tą wyodrębnioną logicznie, nie istniejącą fizycznie przestrzeń tworzy cała treść zawartych w systemach danych, pliki, strony internetowe, aplikacje oraz procesy, do których uzyskujemy dostęp wyłącznie poprzez systemy informatyczne, co stanowi ujęcie znacznie precyzyjniejsze od zaprezentowanego na gruncie amerykańskim. Należy w tym miejscu jednak zaznaczyć, że definicja KE ogranicza zakres przedmiotowy pojęcia do cyfrowej przestrzeni wykorzystywanej przez komputery osobiste (PC – *personal computer*). Ujęcie to oznacza w praktyce zawężenie cyberprzestrzeni do Internetu z dodatkowym jednak zastrzeżeniem wyłączenia obszaru operacji dokonywanych za pomocą wszelkich urządzeń innych od komputerów, które choć przetwarzają te same rodzaje danych informatycznych oraz wykorzystują liczne możliwości Internetu – np. telefony komórkowe, posiadające aktualnie wiele funkcjonalności zbliżonych do komputerów (przetwarzanie plików, funkcje sieciowe), to jednak, zgodnie z przyjętą w informatyce nomenklaturą,

---

[112] Słownik dostępny na stronie internetowej Komisji Europejskiej pod adresem: http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c. W oryginale: „*Virtual space in which the electronic data of worldwide PCs circulate.*".

komputerami nie są[113].

Przygotowany przez Komisję Europejską słownik nie definiując pojęcia „*personal computer*" zmusza jednocześnie do stosowania właśnie potocznego rozumienia tego określenia. Także jako nadmierne uproszczenie potraktować należy fakt zupełnego pominięcia w definicji użytkowników cyberprzestrzeni oraz zachodzących pomiędzy nimi interakcji. Należy jednak zaznaczyć, że ponieważ pojęcie cyberprzestrzeni wciąż nie jest używane na gruncie prawa Unii Europejskiej (nie jest to pojęcie należące do języka prawnego) w praktycznym zastosowaniu w komunikatach lub wiadomościach publikowanych przez organy UE stosowane jest niejednokrotnie dosyć luźno, często pozostawiając wątpliwości, co do rzeczywistego rozumienia tego pojęcia w konkretnym kontekście[114].

W porządkach krajowych poszczególnych państw Europy definicja cyberprzestrzeni wprowadzana jest najczęściej poprzez formułowane na szczeblu rządowym strategie cyberbezpieczeństwa. Samo pojęcie cyberbezpieczeństwa, wywodzące się z anglojęzycznego terminu *cybersecurity* (często pisanego także jako osobne wyrazy *cyber security*) oznacza całokształt działań podejmowanych w celu urzeczywistnienia postulowanego stanu, w którym ryzyka grożące operacjom dokonywanym w cyberprzestrzeni są możliwie zminimalizowane[115]. Przegląd krajowych strategii pod kątem analizy definicji cyberprzestrzeni dokonany został w oparciu o rozwiązania przyjęte w Anglii, Niemczech, Francji, Holandii oraz Polsce.

Spojrzenie brytyjskie przeanalizowane zostało w oparciu o dwa dokumenty rządowe. W wydanej przez brytyjski gabinet w 2009 r. Strategii Cyberbezpieczeństwa Zjednoczonego Królestwa[116] zamieszczona została następująca definicja cyberprzestrzeni:

---

[113] Tak np. http://pl.wikipedia.org/wiki/Komputer_osobisty.

[114] Nawet na gruncie Sprawozdania Komisji dla Rady i Parlamentu Europejskiego z oceny dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE, tzw. Dyrektywa retencyjna) dopuszczalne wydaje się stanowisko, że nowoczesny ruch telefoniczny, w szczególności ten oparty o przesyłanie pakietów danych, również odbywa się w obszarze cyberprzestrzeni: „groźby karalne wysunięte na czatach internetowych nie pozostawiają żadnego innego śladu oprócz danych o ruchu w cyberprzestrzeni. Podobna sytuacja dotyczy przestępstw popełnianych za pośrednictwem telefonu.". Sygnatura dokumentu: *COM/2011/0225 final*, dostępny na stronie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0225:EN:HTML. Co znamienne sama dyrektywa retencyjna nie posługuje się pojęciem cyberprzestrzeni zaś ruch internetowy odróżnia od ruchu telefonicznego jedynie poprzez wskazanie odrębnych identyfikatorów urządzeń końcowych biorących udział w procesie wymiany danych. Innym przykładem może być także wiadomość opublikowana na stronie http://ec.europa.eu/news/environment/080228_1_pl.htm, w treści której po wskazaniu na Internet oraz telefonię komórkową używane jest zastępczo określenie cyberprzestrzeń.

[115] Więcej na ten temat oraz o znanych standardach na stronach: http://www.us-cert.gov/cas/tips/ST04-001.html oraz http://en.wikipedia.org/wiki/Cyber_security_standards.

[116] Strategia Cyber Bezpieczeństwa Zjednoczonego Królestwa - bezpieczeństwo, ochrona oraz odporność w cyber przestrzeni. W oryginale: „Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space". Tłumaczenie własne. Dokument dostępny na stronie internetowej pod adresem: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf.

„Nowa domena komputerowej komunikacji, która jest esencjonalna dla ekonomii, społeczeństwa oraz politycznego zdrowia krajów rozwiniętych. Klockami, z których jest zbudowana są poszczególne komputery oraz systemy komunikacyjne. Te niedostrzegalne elementy techniczne stanowią podbudowę wielu naszych codziennych zajęć, zarówno zawodowych, jak i podejmowanych w życiu prywatnym, ale także w sposób fundamentalny wspierają naszą krajową infrastrukturę oraz przepływ informacji."[117].

Definicję tę znacząco uzupełniają ponadto dwa następujące fragmenty zawarte w strategii. Jako wprowadzenie do zagadnienia definiowania cyberprzestrzeni zapisano, że „Cyberprzestrzeń obejmuje wszelkie formy sieciowej, cyfrowej działalności; zawierają się w tym treść oraz same działania dokonywane poprzez cyfrowe sieci."[118]. W zdaniu otwierającym dokument czytamy zaś, że „Każdego dnia, miliony ludzi w Wielkiej Brytanii opierają się na usługach oraz informacjach, które składają się na cyberprzestrzeń: to jest, wszelkich formach sieciowej, cyfrowej działalności. Mogą oni mieć świadomość tego faktu w czasie surfowania po Internecie, robienia zakupów, czy rozwijania kontaktów za pośrednictwem sieci, ale mogą także nie uświadamiać sobie sieciowej otoczki działalności podbudowującej usługi, na których polegają, czy tego, jak bardzo zależne stało się funkcjonowanie administracji państwowej, biznesu oraz infrastruktury krajowej od tej nowej domeny ludzkiej działalności."[119].

Zaprezentowany powyżej sposób definiowania cyberprzestrzeni kładzie największy nacisk na jej społecznym aspekcie, ukazując tą przestrzeń, jako swojego rodzaju forum ludzkiej aktywności, będące jednocześnie źródłem oraz miejscem realizacji nowoczesnych usług. Na podkreślenie zasługuje tu waga, jaka przypisywana jest tak ujętej cyberprzestrzeni. Strategia wyraźnie wskazuje na ogromne znaczenie domeny zarówno dla sektora

---

117 Strategia Cyberbezpieczeństwa Zjednoczonego Królestwa, s. 3. W oryginale: „*The new domain of computer-facilitated communication that is essential for the economic, social and political health of advanced nations. The physical building blocks of cyber space are individual computers and communications systems. These discrete technical elements underpin many of our daily activities, both at work and in our personal lives, and also fundamentally support much of our national infrastructure and information.*". Tłumaczenie własne.

118 Strategia Cyber Bezpieczeństwa Zjednoczonego Królestwa, s. 7. W oryginale: „*Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks.*". Tłumaczenie własne.

119 Strategia Cyber Bezpieczeństwa Zjednoczonego Królestwa, s. 7. W oryginale: „*Every day, millions of people across the United Kingdom rely on the services and information that make up cyber space: that is, all forms of networked, digital activities. They may be aware of this if surfing the web, shopping or social networking online, or they may be unaware of the networked activity underpinning the services they rely on, and of just how critically dependent the work of government, business and national infrastructure is on this new domain of human activity.*". Tłumaczenie własne.

prywatnego[120], jak i publicznego, co znamienne, podkreślając również polityczną rolę cyberprzestrzeni. Cyberprzestrzeń została tu określona jako domena komunikacji, co może prowadzić do wniosku, że działanie niepolegające na przesyłaniu danych, nie stanowi działania w cyberprzestrzeni. Z drugiej strony, wskazując na elementy fizycznej infrastruktury tworzącej technologiczne podwaliny cyberprzestrzeni, definicja wymienia w tym zakresie poszczególne (pojedyncze) komputery oraz systemy komunikacyjne, do których zalicza się także nowoczesne sieci telefoniczne. Wyraźne wskazanie „poszczególnych komputerów" oraz odróżnienie ich od systemów komunikacyjnych równolegle uprawnia zatem przyjęcie założenia, że na gruncie definicji, także operacje wykonywane w obrębie tylko jednego systemu również mogą stanowić działanie w cyberprzestrzeni, choć z konieczność logicznej, nie mogą one polegać na przesyłaniu danych. Powstające na tym tle wątpliwości należy zatem ocenić negatywnie, jako dopuszczające sprzeczne interpretacje poszczególnych fragmentów definicji w kwestii zasługującej na wyraźne, precyzyjne rozstrzygnięcie. Warstwa programowa cyberprzestrzeni pozostawiona została natomiast w całości w domyśle. Co niezwykle ważne, poruszając zagadnienie budowy infrastrukturalnej, strategia zwraca szczególną uwagę na transparentność technologii cyberprzestrzeni. Złożoność nowoczesnych rozwiązań sieciowych ukrywana jest dziś pod przyjaznymi dla użytkowników interfejsami oprogramowania, których zadaniem jest umożliwianie łatwego wykorzystywania nowych możliwości teleinformatycznych bez konieczności poznania ich technicznej budowy. Idea ta wymaga wyraźnego podkreślenia bowiem w praktyce to właśnie ta cecha cyberprzestrzeni – sprowadzająca się do prostoty uczestnictwa – stała się jednym z filarów jej gwałtownego rozwoju na tak różnych obszarach działalności społecznej. Jednocześnie, wprowadzenie do zaawansowanych technologicznie sieci użytkowników, którzy pozostają zupełnie nieświadomi zasad ich funkcjonowania stało się jedną z głównych przyczyn pojawienia się elektronicznych nadużyć oraz popularyzacji tego zjawiska do masowej wręcz skali. Wciąż bowiem świadomość możliwości sieciowych oraz płynących z tej strony zagrożeń jest wśród „zwyczajnych" użytkowników uplasowana na bardzo niskim poziomie, co powoduje, że stanowią oni prosty cel dla cybernetycznych ataków, padając ofiarami napaści, z których zajścia niejednokrotnie wręcz w ogóle nie zdają sobie sprawy.

W dwa lata od ukazania się wskazanego wyżej dokumentu – a więc w roku 2011,

[120] W Strategii wskazano między innymi na ogromny obrót dokonywany za pośrednictwem Internetu – jeszcze w 2009 r. wartość rocznej sprzedaży dokonanej przez Brytyjczyków *on-line* przekroczyła 50 miliardów funtów, źródło: *Digital Britain: The Final Report* 2009 (Cm 7650), Strategia Cyberbezpieczeństwa Wielkiej Brytanii, s. 8.

brytyjski gabinet wydał następnie drugą strategię cyberbezpieczeństwa, której pełny tytuł przyjął brzmienie „Strategia Cyber Bezpieczeństwa Zjednoczonego Królestwa - ochrona oraz promocja Zjednoczonego Królestwa w cyfrowym świecie”[121]. Zawarta w późniejszej strategii definicja pojęcia „cyberprzestrzeń”, choć w żadnej mierze nie przekreśliła sensu definicji wcześniejszej również utrzymując spojrzenie społeczno-ekonomiczne, została jednak uzupełniona o istotne elementy. Dwa lata doświadczeń skłoniły rząd brytyjski do wprowadzenia do strategii następującego *definiens* dla cyberprzestrzeni:

> „Cyberprzestrzeń to interaktywna domena stworzona z cyfrowych sieci, która wykorzystywana jest do przechowywania, modyfikowania oraz przekazywania informacji. Jej częścią jest Internet, ale zawierają się w niej także inne systemy informacyjne, które obsługują nasz biznes, infrastrukturę oraz wspomagają świadczenie usług. Cyfrowe sieci już dziś podbudowują proces zaopatrywania naszych domów w energię elektryczną oraz wodę, pomagają organizować dostawy żywności oraz innych dóbr do sklepów oraz służą za niezbędne narzędzie biznesowe w całym Zjednoczonym Królestwie. Ich zasięg ustawicznie się powiększa, w miarę jak podłączamy do nich nasze telewizory, konsole do gier, czy nawet urządzenia AGD.”[122].

W tym miejscu, skupiając się jedynie na nowych elementach definicji, w pierwszej kolejności wskazać należy wyraźne wprowadzenie do definicji Internetu, jako jednej (głównej) z sieci składającej się na obszar cyberprzestrzeni. Definicja nie ogranicza jednak swojego zakresu tylko do tej sieci rozległej, nie wyłączając z cyberprzestrzeni innych sieci – a zatem odseparowanych od sieci WWW, jak np. sieci lokalne wykorzystywane w dużych przedsiębiorstwach (tzw. intranet). Wprowadzenie pojęcia interaktywności podkreśla istotną cechę sieci, która w odróżnieniu np. od telewizji, jest dla swoich użytkowników nie tylko funkcjonującym jednostronnie źródłem informacji, ale także obszarem, który – choćby częściowo - podlega również woli użytkowników, wykonując zadane operacje. Wyliczenie funkcjonalności cyberprzestrzeni – przechowywanie, modyfikowanie oraz przekazywanie informacji, usuwa natomiast wcześniejsze wątpliwości, powstające na gruncie pierwszej

---

[121] Strategia Cyber Bezpieczeństwa Zjednoczonego Królestwa - ochrona oraz promocja Zjednoczonego Królestwa w cyfrowym świecie. W oryginale:” The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world.”. Tłumaczenie własne. Tekst dostępny na stronie internetowej pod adresem: http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

[122] Strategia Cyber Bezpieczeństwa Zjednoczonego Królestwa (z 2011 r.), s. 10. W oryginale: „*Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services. Digital networks already underpin the supply of electricity and water to our homes, help organise the delivery of food and other goods to shops, and act as an essential tool for businesses across the UK. And their reach is increasing as we connect our TVs, games consoles, and even domestic appliances.*”. Tłumaczenie własne.

definicji, co do charakteru działań niepolegających na przesyłaniu danych, dokonywanych w obrębie jednego systemu. W rozumieniu późniejszej definicji zatem nie tylko komunikacja stanowi działanie w cyberprzestrzeni. Jako przeoczenie ocenić należy natomiast niewskazanie w katalogu funkcjonalności także samego wytwarzania informacji. Jednocześnie, wskazanie na cyfrowe sieci jako element infrastrukturalny cyberprzestrzeni, zastępujący użyte w poprzedzającej definicji „poszczególne komputery oraz systemy komunikacyjne", oznacza, że pojedynczy system, odseparowany od jakiejkolwiek sieci, nie może być na gruncie omawianej tu definicji włączony do zasięgu cyberprzestrzeni. Wyrazem najnowszych trendów podłączania do sieci coraz to nowych kategorii urządzeń, stało się natomiast ostatnie zdanie przytoczonej definicji, w którym, jako ciekawostkę, wskazano także na konsole do gier video. O ile w Europie rynek gier nie jest jeszcze tak wyraźnie zaznaczony, o tyle w USA, Japonii czy Korei Południowej, zyski w tym obszarze sięgają miliardów dolarów, zaś wyniki sprzedaży jednego tylko tytułu przekraczają nierzadko dziesiątki milionów egzemplarzy[123].

Inaczej niż w przedstawionym podejściu brytyjskim, rozłożone zostały akcenty w opracowaniu kontynentalnym, sporządzonym w ramach prac nad Strategią Cyber Bezpieczeństwa dla Niemiec z 2011 r.[124]. Zawarta w tym dokumencie definicja cyberprzestrzeni, określa tę domenę w następujący sposób:

> „Cyberprzestrzeń jest wirtualną przestrzenią wszystkich systemów technologii informacyjnej powiązanych na poziomie danych w skali globalnej. Fundament cyberprzestrzeni stanowi Internet, jako uniwersalna oraz powszechnie dostępna sieć oferująca połączenia oraz transport, która może być uzupełniania oraz rozszerzana dalej przez dowolną ilość dodatkowych sieci danych. Systemy IT działające w wyizolowanej przestrzeni wirtualnej nie stanowią części cyberprzestrzeni."[125].

Spojrzenie to, inaczej od angielskiego, skupia się na kwestiach technologicznych, kładąc nacisk na zagadnieniach, kolejno, określenia zasięgu logicznego cyberprzestrzeni oraz opisu obsługującej ją infrastruktury. Punktem wyjścia, podobnie jak w definicji Komisji

---

[123] Dla przykładu, popularna w Stanach Zjednoczonych Ameryki gra *World of Warcraft* pod koniec roku 2011 miała prawie dziesięć i pół miliona aktywnych użytkowników opłacających miesięczny abonament. Gra uzyskała oficjalny wpis do Księgi Rekordów Guinessa (za: http://en.wikipedia.org/wiki/World_of_Warcraft). Inna głośna seria gier zatytułowana *Halo* (części 1 - 3) wygenerowała natomiast światową sprzedaż o wartości dwóch miliardów dolarów, sprzedając się w ponad 40 milionach egzemplarzy (za: http://en.wikipedia.org/wiki/Halo_(series)) .

[124] Strategia Cyber Bezpieczeństwa dla Niemiec. W oryginale: „*Cyber Security Strategy for Germany.*". Dokument w wersji anglojęzycznej dostępny na stronie internetowej pod adresem: http://www.cio.bund.de/SharedDocs/ Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.

[125] W oryginale: „*The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.*". Tłumaczenie własne.

Europejskiej jest tu *przestrzeń wirtualna*, czyli nie istniejący fizycznie obszar, będący *binarną* domeną logiczną, w której przetwarzane są informacje (przestrzeń nie w rozumieniu fizycznym, ale przestrzeń jako idea). Definicja precyzuje przy tym, że fizyczną podstawą tej domeny są sieci, w tym przede wszystkim Internet, łączące pojedyncze fragmenty wirtualnej przestrzeni (tworzonej np. przez pojedyncze komputer każdego z nas) w jeden globalny obszar. Jak podkreślono w definicji, systemy odseparowane od tego światowego udziału pozostają wyłączone z definiowanej tu cyberprzestrzeni.

Ujęcie niemieckie choć wskazując na Internet jako podstawę cyberprzestrzeni, nie ogranicza jej zasięgu wyłącznie do tej sieci oraz elementów ją tworzących, wskazując jednocześnie na niezwykle ważną cechę nowoczesnych sieci teleinformatycznych – rozszerzalność. Tak definiowane pojęcie cyberprzestrzeni zawiera zatem w sobie wszystkie rodzaje sieci łączących urządzenia służące do przetwarzania danych (w tym więc również sieci telefoniczne), ale także zwraca uwagę na ustawiczny rozrost opisywanego obszaru, postępujący na wskutek podłączania do sieci globalnej coraz to kolejnych sieci lokalnych, co powoduje włączanie zasobów tych drugich do ogólnoświatowej domeny. Powstaje w ten sposób rodzaj pajęczyny, w której z punktu widzenia jej działania, całość składa się z setek tysięcy mniejszych podsieci wzajemnie ze sobą połączonych, potrafiących jednak stworzyć jeden wspólny organizm, kierujący się swoją wewnętrzną logiką sieciową[126]. Logika ta, stanowiąc jedną z podstawowych cech paradygmatu nowoczesnych technologii, wyraża się w szczególnej morfologii sieci, pozwalającej nie tylko na jej ustawiczny rozrost, ale także ciągłe dostosowywanie się do nowych możliwości oraz potrzeb. Wspomniana w definicji rozbudowa sieci, obejmująca tak rozszerzanie topologiczne, jak i funkcjonalne oparte na twórczym potencjale nowych form interakcji, musi bowiem utrzymywać atrybuty strukturyzacji, bez której sieć nie mogła by funkcjonować jako całość budowana niezależnie z małych części. Jednocześnie jednak, rozbudowa ta musi zachowywać odpowiedni poziom elastyczności, niezbędny dla zapewnienia dalszego rozwoju[127]. W ujęciu tym, ogólnoświatowe sieci stanowią więc rodzaj cyfrowej tkanki cyberprzestrzeni, w której pojęcie jednolitości zastąpione zostało minimalizacją porządku, wprowadzanego wyłącznie w zakresie niezbędnym do funkcjonowania tej przestrzeni jako całości w skali globalnej. Na gruncie technologicznym, cechy te zarysowują się szczególnie wyraźnie w zasadach adresacji sieci, pozwalających każdemu z nas na rozszerzenie zasobów Internetu poprzez podpięcie za pośrednictwem własnego komputera dowolnej podsieci, która tym samym stanie

[126] M. Castells, Społeczeństwo sieci, Wydawnictwo Naukowe PWN, Warszawa 2010, s. 103.
[127] *Ibidem,* s. 103.

się dostępna z całego świata – wykorzystując jedynie podstawową wiedzę na temat sieci możemy nie tylko udostępniać pliki fizycznie znajdujące się na dysku naszego komputera, ale także umożliwić np. wydrukowanie na domowej drukarce dokumentu człowiekowi obsługującemu komputer na drugim końcu świata. Sieciowa logika charakteryzująca się minimalizmem porządku wyraża się ponadto w niezwykłych zdolnościach sieci do inkorporowania nowych funkcjonalności programowych oraz rozwoju infrastruktury sieciowej przy zachowaniu jej wewnętrznej spójności oraz kompatybilności. Pomimo globalnej skali Internetu, sieć ta podlega ustawicznej rozbudowie oraz ewolucji bez odgórnego wyznaczania jej jakichkolwiek kierunków. Warto zauważyć, że tempo tego rozwoju znacznie przekracza możliwości adaptacyjne znane w świecie naturalnym. Podstawy technologiczne budowy rozległych sieci, w szczególności zaś Internetu, stanowiące istotne uzupełnienie dla rozważań na temat budowy oraz funkcjonowania cyberprzestrzeni, zostały przedstawione szerzej w kolejnych częściach pracy.

Zgodnie z zaproponowanym tokiem analizy, w tym miejscu należy przenieść rozważania na grunt francuski. Kolejna z definicji cyberprzestrzeni wywodzących się z europejskich strategii cyberbezpieczeństwa zawarta została w dokumencie przygotowanym w 2011 r. przez Francuską Agencję Bezpieczeństwa Sieci oraz Informacji (ANSSI)[128] - zatytułowanym „Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji”[129]. Sformułowana tam definicja cyberprzestrzeni, określiła ją lakonicznie jako:

> „Przestrzeń komunikacyjna utworzona przez globalne połączenie sprzętu służącego do automatycznego przetwarzania cyfrowych danych”[130].

Definicja francuska nie porusza tym samym bezpośrednio ani kwestii dotyczących użytkowników, ani szerszego spektrum zjawisk społecznych, czy ekonomicznych, skupiając się w całości na określeniu cyberprzestrzeni jako przestrzeni komunikacyjnej bazującej na infrastrukturze rozsianej po całym świecie. Jednocześnie, dotykając podstaw

---

[128] *Agence nationale de la sécurité des systèmes d’information* (ANSSI). Oryginalne tłumaczenie angielskie brzmi zaś: “French Network and Information Security Agency” (FNISA). Oficjalna strona internetowa Agencji dostępna jest pod adresem : www.ssi.gouv.fr. ANSSI prowadzi także portal poświęcony zagadnieniom bezpieczeństwa informatycznego, znajdujacy się pod adresem www.securite-informatique.gouv.fr. Informacje o Agencji można znaleźć także na stronie internetowej pod adresem: http://fr.wikipedia.org/wiki/Agence_nationale_de_la_s%C3%A9curit%C3%A9_des_syst%C3%A8mes_ d'information.

[129] Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji. W oryginale: *„Défense et sécurité des systèmes d’information. Stratégie de la France*”. Tłumaczenie własne. Dokument dostępny na stronie internetowej pod adresem: http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011.

[130] Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji, s. 21. W oryginale: „*Espace de communication constitué par l’interconnexion mondiale d’équipements de traitement automatisé de données numériques.*”. Tłumaczenie własne.

technologicznych, definicja nie tyle wskazuje na same elementy sieci, konkretne rodzaje urządzeń wchodzących w jej skład, czy składniki warstwy programowej, co odwołuje się do technologicznego połączenia o globalnym zasięgu, scalającego w jedność wszelki sprzęt przetwarzający cyfrowe dane. Pod tym ostatnim pojęciem należy rozumieć zarówno elementy sieci komputerowych, jak i telekomunikacyjnych, a więc definicja nie ogranicza poruszania się w cyberprzestrzeni jedynie do sfery przetwarzania danych na komputerach.

Tak ujęta cyberprzestrzeń przedstawia koncepcję pustego obszaru, który wypełniają składniki niewymienione w definicji: wszelkie działania użytkowników, świadczone na ich rzecz usługi, relacje pomiędzy nimi itd. Podstawą tego obszaru jest jednak komunikacja, stanowiąca w prezentowanej definicji istotę cyberprzestrzeni. Zasadne na gruncie tak sformułowanej definicji jest tym samym postawienie tezy, że działając tam, gdzie nie zachodzi komunikacja pomiędzy zakończeniami sieci - czy to komputerami, telefonami, czy innymi urządzeniami umożliwiającymi łączność oraz wymianę danych, nie możemy mówić o poruszaniu się w cyberprzestrzeni. Rozumienie to zbieżne jest z prezentowanym wcześniej na gruncie definicji niemieckiej. W tym miejscu podkreślenia wymaga jednak fakt, iż komunikacja, na którą wskazuje się w definicji francuskiej, nie wymaga w sposób wyraźny bezpośredniego udziału człowieka, a zatem może dotyczyć także w pełni zautomatyzowanej wymiany danych pomiędzy odpowiednio skonfigurowanymi urządzeniami („globalne połączenie sprzętu służącego do automatycznego przetwarzania”). Ujęcie niemieckie nie dotykając samej komunikacji pozostawiało natomiast tę kwestię poza zasięgiem rozważań. Ten nowy element pozwala jednak zwrócić uwagę na szczególną rolę technologii, która nie tylko tworzy cyberprzestrzeń, ale w pewnym zakresie stanowi także jednego z jej użytkowników, np. w sytuacji, gdy niezależne urządzenia łączą się ze sobą celem optymalizacji swojej pracy i przyspieszenia obsługi użytkowników.

Francuska strategia cyberbezpieczeństwa dostarcza jednak także wielu innych ciekawych wniosków na temat cyberprzestrzeni, nieujętych wprost w samej definicji pojęcia zawartej w dokumencie. Socjologicznym rozwinięciem koncepcji cyberprzestrzeni, jako obszaru komunikacji o zasięgu światowym jest nazwanie jej „Nową Wieżą Babel”[131]. Cyberprzestrzeń nie tylko zbliża, czy pozwala współdzielić, ale wręcz powoduje mieszanie się kultur gromadząc na bieżąco idee oraz informacje pochodzące z całego świata. Stwierdzenie, że wyłączenie się z niej powoduje izolację jednostek, spadek konkurencyjności przedsiębiorstw oraz podrzędność krajów[132] wskazuje na ogromną rolę tego obszaru,

[131] Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji, prolog.
[132] Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji, prolog. W oryginale:

określającą go jako główny nurt dla uczestniczenia w nowoczesnej, globalnej społeczności.

Innym równie interesującym określeniem użytym w strategii francuskiej jest także nazwanie cyberprzestrzeni „Nowymi Termopilami”, gdzie na co dzień dochodzi do niewidocznych w świecie materialnym starć, nie tylko zaburzających poprawne funkcjonowanie systemów, naruszających dobra prawne ich użytkowników, ale także mogących zagrozić ludzkiemu życiu, gdy np. atakowane są systemy odpowiedzialne za szeroko rozumiane bezpieczeństwo publiczne. Niepodważalne stało się dziś bowiem zjawisko przeskoku pomiędzy działaniami w cyberprzestrzeni a skutkami występującymi w świecie fizycznym[133]. Dodając do tego globalny zasięg cyberprzestrzeni, umożliwiający podejmowanie wrogich działań w odległych krajach, w dodatku za pośrednictwem systemów zlokalizowanych w państwach trzecich, Strategia formułuje postulat zacieśniania współpracy międzynarodowej dla prawnego ugruntowania wspólnej walki z nowoczesnymi zagrożeniami. Ponadgraniczność cyberprzestrzeni, będąca immanentną cechą tego obszaru, musi bowiem zostać uwzględniona także na gruncie stosunków międzypaństwowych, które stają się szczególnie delikatne w kwestiach władzy oraz jurysdykcji. Idea globalnej wioski jako zjawiska opisującego łączenie odległych społeczeństw na płaszczyźnie zarówno ekonomicznej, jak i kulturowej, którego głównym motorem rozwoju jest dzisiaj cyberprzestrzeń – z każdym dniem coraz wyraźniej wpływa na postrzeganie podstaw nowoczesnej państwowości.

Na tle powyżej przybliżonych definicji cyberprzestrzeni, umieszczonych w strategiach Anglii, Niemiec oraz Francji, jako rozwiązanie odbiegające od przyjętego w Europie nurtu określania tego cyfrowego medium należy przedstawić koncepcję przyjętą w opracowaniu przygotowanym przez Holandię. W wydanej w tym kraju w 2011 r. strategii cyberbezpieczeństwa[134] pojęcie cyberprzestrzeni (stanowiące przecież logiczną oś dla cyberstrategii w przypadku innych krajów) postanowiono w ogóle usunąć oraz zastąpić innym określeniem odwołującym się do oznaczenia nowoczesnych technologii informacyjnych. Obszar, którego bezpieczeństwo stało się celem wprowadzenia holenderskiej strategii, określony został w tym przypadku skrótem ICT[135] (Technologia Informacyjna oraz

---

„L'exclusion du numérique condamne les individus à l'isolement, les entreprises à la décroissance et les nations à la dépendance.”.

[133] W Strategii czytamy o potencjalnych lub faktycznych konsekwencjach przeskoku pomiędzy sferami cyfrową oraz „ludzką”. W oryginale: *„les conséquences potentielles ou réelles de l'imbrication entre le numérique et l'activité humaine.”*.

[134] Krajowa Strategia Cyberbezpieczeństwa. Sukces poprzez współpracę. W oryginale: “*The National Cyber Security Strategy (NCSS). Success through cooperation.*”. Dokument dostępny na stronie internetowej pod adresem: http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.

[135] Skrót ten, choć stosowany rzadko, znany jest w świecie języka informatycznego oraz rozwija się w oryginale

Komunikacyjna), zdefiniowanym w dokumencie jako:

„Ogół cyfrowych informacji, informacyjnej infrastruktury, komputerów, systemów, oraz oprogramowania, a także interakcje zachodzące pomiędzy technologią informacyjną, a światem fizycznym, w odniesieniu do których następuje proces komunikacji oraz wymiany informacji."[136].

Zakresowo powyższa definicja łączy w sobie wybrane elementy znane z wcześniej wymienionych strategii, jak informacje, infrastruktura, czy ogólnie ujmując – wszelkie zależności pomiędzy światem cyfrowym a fizycznym. Jakie zatem różnice wynikają z przyjęcia w przedstawionej definicji koncepcji pozbawionej określenia „cyberprzestrzeń" oraz intencjonalnego zastosowania w tym przypadku innego nazewnictwa?

Ujęcie holenderskie w swojej odmienności zwraca uwagę brakiem wyraźnej, prostej implementacji idei wytworzenia nowej, odrębnej, cyfrowej domeny ludzkich działań. Nie ma tu znanych z przytoczonych wcześniej definicji „cyberprzestrzeni" odwołań do „domeny komunikacji", „wirtualnej rzeczywistości", czy „przestrzeni komunikacyjnej", zaś samo *definiendum* pozbawione jest członu „przestrzeń".

Przyjęta w analizowanej strategii bezpieczeństwa definicja ICT wskazuje w pierwszej kolejności na technologiczną podstawę wymiany cyfrowych informacji wraz z jej atrybutami fizycznymi, stanowiącymi elementy infrastrukturalne dla systemu komunikacji oraz same informacje zapisane w postaci cyfrowej. Po pierwsze zatem, ICT to wszelkie technologie sprzętowe oraz programowe umożliwiające przetwarzanie oraz wymianę informacji wraz z tymi informacjami zapisanymi w formacie cyfrowym, na informatycznych nośnikach danych. Druga część definicji uzupełnia natomiast desygnaty definiowanego pojęcia poprzez wprowadzenie konstrukcji interakcji pomiędzy technologią informacyjną a światem fizycznym. Interakcje te, choć niesprecyzowane w definicji odnośnie formy, należy przyjąć, że mogą zachodzić w obydwu kierunkach, wytwarzając swojego rodzaju wzajemną zależność pomiędzy triadą elementów infrastruktury technologii informacyjnej, przetwarzanych w nich

---

jako „*Information and Communications Technology*" (Technologia Informacyjna oraz Komunikacyjna). Uważa się go za rozwinięcie oraz dopełnienie popularnego określenia „IT" – „*Information Technology*", oznaczającego wprost jedynie technologie informacyjne, jednak w praktyce stosowanego także w odniesieniu do technologii komunikacji. Termin „ICT" używany jest najczęściej w kontekście wskazywania konwergencji usług (łączenie usług teleinformatycznych, telekomunikacyjnych na jednej platformie, np. telewizja, Internet oraz telefon na jednym łączu od jednego dostawcy). Jako autora określenia „ICT" traktuje się Dennisa Stevenson'a, który posłużył się nim po raz pierwszy w 1997 roku. Źródło: http://en.wikipedia.org/wiki/Information_and_ communication_technologies#cite_note-3.

[136] Krajowa Strategia Cyberbezpieczeństwa. Sukces poprzez współpracę, s. 2. W oryginale: „*ICT is the entirety of digital information, information infrastructures, computers, systems, applications and the interaction between information technology and the physical world regarding which there is communication and information exchange.*". Tłumaczenie własne.

zasobami - czyli informacjami, oraz społeczeństwem, nazywanym także w strategii „społeczeństwem cyfrowym".

Nieco niekonsekwentnie do wskazanego na wstępie wyraźnego braku odwołania się w definicji do idei wytworzenia nowej przestrzeni, strategia wskazując na „świat fizyczny" sugeruje jednak domniemanie, że w zakresie technologii informacyjnych istnieje także swojego rodzaju przestrzeń „nie-fizyczna", stanowiąca jedynie konceptualną przestrzeń przetwarzania informacji występujących w czystej postaci, jako pewne idee, a więc w oderwaniu od ich fizycznego substratu (nośnika) – można sądzić, że w tym także od formy zapisu cyfrowego. Po drugie więc, pod pojęciem ICT należy rozumieć sumę wszelkich możliwych zależności pomiędzy funkcjonowaniem systemów teleinformatycznych, kreujących swojego rodzaju podstawę do niezakłóconej wymiany informacji (na poziomie sprzętowym – wymianę danych) a funkcjonowaniem nowoczesnych społeczeństw cyfrowych. Są to zależności o charakterze nie tylko technologicznym, ale także społecznym, których skutki sięgają daleko poza systemy teleinformatyczne. Jako przykłady takich zależności dokument wskazuje między innymi na współczesne zagrożenia dla funkcjonowania sieci, jak wirusy komputerowe, czy ataki *denial of service* (dos), które choć występują w systemach w postaci cyfrowej, wpływają na fizyczną infrastrukturę sieci mogąc spowodować jej *realne* uszkodzenia. W zakresie powiązań ekonomii oraz teleinformatyki strategia podnosi kwestię wzrostu gospodarczego, który uzależniony jest aktualnie od stosowania nowoczesnych rozwiązań teleinformatycznych, a zgodnie z przedstawionymi w dokumencie badaniami, aż 50 % wzrostu produkcji w Europie stanowi wynik stosowania ICT. Jednocześnie, możliwości świadczenia nowych rodzajów usług (które powstały np. dzięki Internetowi) wiążą się automatycznie z nowymi zagrożeniami, tak dla usługodawców, jak i usługobiorców. Wreszcie, w zakresie społecznym, strategia wskazuje na postępujący proces cyfryzacji społeczeństwa, wiążący się przetwarzaniem w systemach ogromnych ilości danych osobowych oraz tworzenie się tzw. mediów społecznych[137], nawiązujących do idei wytworzenia niczym nieograniczonej, ani nie skrępowanej platformy wymiany informacji przez użytkowników, zarówno w skali mikro (tylko ze znajomymi), jak i makro (z całym światem)[138].

---

[137] W oryginale *Social Media*. Termin odnosi się do wykorzystywania nowoczesnych środków komunikacji (przede wszystkim Internetu) jako medium służącego użytkownikom do tworzenia oraz wymiany informacji, w postaci swoistego cyfrowego dialogu. Tak zdefiniowane media społeczne, stanowią nowoczesną bazę dla wszelkich społecznych interakcji. Przykładami konkretnych rozwiązań są m.in. wszelkie portale społecznościowe, jak Facebook, Youtube, Twitter, czy choćby nowoczesne encyklopedie internetowe tworzone przez wszystkich użytkowników. Źródło: http://en.wikipedia.org/wiki/Social_media.

[138] Krajowa Strategia Cyberbezpieczeństwa. Sukces poprzez współpracę, s. 2 i 3.

Zamykając powyższą analizę, przy identyfikacji różnic występujących pomiędzy ujęciami zawartymi w strategii holenderskiej a pozostałymi strategiami europejskimi, wskazać należy na dwie główne kwestie. Po pierwsze, pominięcie bezpośredniego odwołania się do obszaru cyberprzestrzeni upraszcza definicję, czyniąc ją lepiej zrozumiałą dla osób niezaawansowanych w arkanach informatyki, co z pewnością też częściowo wynika z funkcji jaką pełnić ma strategia krajowa jasno wyznaczająca swoje cele. Po drugie zaś, strategia holenderska stawiając nacisk na interakcje zachodzące pomiędzy technologią informacyjną a światem fizycznym, sugeruje swojego rodzaju mierzalność tych interakcji, przypominając, że koniec końców, każda wymiana informacji zachodzi pomiędzy identyfikowalnymi użytkownikami w rzeczywistym świecie. Tym samym, definicja holenderska jest wyrazem odejścia, choć nie w pełni konsekwentnego, od trudnej koncepcji istnienia nowego obszaru (cyfrowej domeny) na rzecz podkreślenia służebnej roli ICT stanowiącej jedynie medium do komunikacji.

Z jednej strony, podejście takie pozwala zachować właściwą perspektywę, ukazującą nowoczesne technologie „na swoim miejscu", istniejące dla ludzi, a nie odwrotnie. Z drugiej jednak, porzucenie koncepcji cyberprzestrzeni, jako obszaru który cechuje się swoimi wyjątkowymi właściwościami, między innymi wyrażającymi się w faktycznym wykreowaniu domeny funkcjonującej ponad granicami państwowymi, skutkuje pozbawieniem się narzędzia do prowadzenia dogłębnej analizy tego, co dzieje się aktualnie w rozległych sieciach teleinformatycznych, jak np. Internet. Inkorporacja pojęcia „cyberprzestrzeń" do języka prawnego oraz prawniczego - a w konsekwencji do rozważań prawniczych, pozwala bowiem na znaczne podwyższenie precyzji badań nad nowoczesnymi formami przestępczości pod kątem zarówno określania kwalifikacji prawnej czynów przestępnych, jak i dokonywania wszelakich ocen prawnoprocesowych niezbędnych dla zachowania poprawnego toku ścigania karnego.

2. Regulacje w polskim porządku prawnym

Na tle wskazanych powyżej inicjatyw państw europejskich, także Polska podjęła starania o sporządzenie swojej krajowej strategii cyberbezpieczeństwa, w której za jeden z niezbędnych elementów uznano definicję samego pojęcia „cyberprzestrzeń". Stworzona jako swojego rodzaju punkt wyjściowy do dalszej debaty pierwsza polska definicja uległa następnie pewnym modyfikacjom, by ramach późniejszego procesu legislacyjnego w końcu znaleźć się w ustawie, choć niestety nie karnej, czyniąc jednak tym samym analizowane pojęcie terminem należącym do sfery języka prawnego, a zatem języka pierwszego stopnia.

Wypada zatem prześledzić drogę, która doprowadziła do stworzenia pierwszych polskich definicji cyberprzestrzeni, w tym pierwszej krajowej definicji legalnej, zawartej w powszechnie obowiązującym akcie normatywnym.

Pierwszym dokumentem należącym do polskiego porządku prawnego, w którym posłużono się pojęciem „cyberprzestrzeń", jednocześnie prezentując definicję tego nowego, nieznanego dotąd terminu, stał się przygotowany pod auspicjami Ministerstwa Spraw Wewnętrznych i Administracji (jako ministerstwa właściwego do spraw informatyzacji) Rządowy program ochrony cyberprzestrzeni RP na lata 2009 – 2011[139]. Dokument został przyjęty w dniu 9 marca 2009 r. przez Komitet Stały Rady Ministrów, wskazując jako jeden z głównych powodów jego sporządzenia, konieczność wzmocnienia ochrony infrastruktury krytycznej kraju przed atakami o charakterze terrorystycznym, w tym cyberterrorystycznym. Dla potrzeb opisu programu, zdefiniowano w nim dwa pojęcia, mianowicie „cyberprzestrzeń" oraz „cyberprzestrzeń RP". Definicje, zbudowane w sposób opisowy, przyjęły, odpowiednio następujące brzmienia:

> „W niniejszym dokumencie cyberprzestrzeń rozumiana jest jako przestrzeń komunikacyjna tworzona przez system powiązań internetowych."[140], oraz
>
> „Jako cyberprzestrzeń państwa przyjmuje się przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa. Cyberprzestrzeń państwa w przypadku Polski określana jest również mianem cyberprzestrzeni RP. Cyberprzestrzeń RP obejmuje między innymi systemy, sieci i usługi teleinformatyczne o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa, system bankowy, a także systemy zapewniające funkcjonowanie w kraju transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemy informatyczne ochrony zdrowia, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne."[141].

Dopiero łączna analiza przedstawionych wyżej pojęć pozwala na przybliżenie, czym - zgodnie z pierwszą krajową próbą określenia omawianego pojęcia, była w istocie cyberprzestrzeń.

---

[139] Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia (w stosowanym w programie skrócie – RPOC 2009-2011). Tekst dostępny stronie internetowej pod adresem: http://www.mswia.gov.pl/portal/pl/2/6966/Zalozenia_do_Rzadowego_programu_ ochrony_cyberprzestrzeni_RP_na_lata_20092011.html.

[140] RPOC 2009-2011, s. 4.

[141] RPOC 2009-2011, s. 4.

W pierwszej kolejności, podkreślenia wymaga fakt, iż jako *genus* w definicji cyberprzestrzeni, przyjęto wyrażenie „przestrzeń", wskazujące na przyjęcie szeroko uznanej w Europie koncepcji cyberprzestrzeni rozumianej, jako swojego rodzaju *miejsce*, stanowiące wirtualną, nienamacalną domenę, którą zarówno odwiedzać, jak i badać można jedynie za pośrednictwem narzędzi teleinformatycznych, w praktyce przede wszystkim podłączonego do sieci komputera. Pojęcie przestrzeni, zostało dookreślone tu przy użyciu przymiotnika „komunikacyjna", co po pierwsze wskazuje na cel stworzenia tej przestrzeni – umożliwienie wymiany danych, a po drugie – wskazuje jej niezbędną cechę.

Przestrzeń odseparowana, to znaczy taka, w której z konieczności logicznej nie jest możliwa żadna komunikacja, nie może tym samym być w świetle omawianej definicji nazywana cyberprzestrzenią. Założenie integralności cyberprzestrzeni było również elementem wcześniej opisanych definicji, pochodzących z cyberstrategii Niemiec[142], Francji[143] oraz późniejszej strategii Anglii[144]. Ponadto, w pełni zgodnie z definicją francuską, interpretacja językowa omawianej definicji z RPOC 2009 – 2011 narzuca także założenie, że w cyberprzestrzeni podejmowane są dopiero te informatyczne operacje na danych, które polegają na ich przekazywaniu, a więc realizowane są w obszarze pomiędzy dwoma, lub większą liczbą systemów teleinformatycznych. Samo zapisywanie danych (wytwarzanie informacji) nie stanowi zatem w tym przypadku działania w cyberprzestrzeni.

Określając budulec tak wyodrębnionej przestrzeni, omawiana definicja wskazywała jedynie na „system powiązań internetowych". Z uwagi na brak bliższego odwołania w jej treści do infrastruktury fizycznej, na gruncie definicji „cyberprzestrzeni" pochodzącej z Rządowego programu, nie było jednak możliwe dokonanie jednoznacznego stwierdzenia, czy pojęcie „systemu powiązań" należy odnosić wyłącznie do zależności o charakterze logicznym, samej wymiany danych – czyli zestawiania połączeń pomiędzy systemami podłączonymi do Internetu, czy także do elementów infrastrukturalnych oraz tworzących przez nie powiązań, w przypadku Internetu łączących serwery za pośrednictwem całej skomplikowanej infrastruktury sieci szkieletowej[145]. Uzupełnienia tej kwestii szukać należało jednak w drugiej z przytoczonych definicji, to jest definicji „cyberprzestrzeni państwa", zwanej w dokumencie, w przypadku państwa Polskiego „cyberprzestrzenią RP". Pojęcie to obejmowało już wyraźnie systemy, sieci i usługi teleinformatyczne zapewniające

[142] Strategia Cyber Bezpieczeństwa dla Niemiec.
[143] Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji.
[144] Strategia Cyber Bezpieczeństwa Zjednoczonego Królestwa (z 2011 r.).
[145] Terminem tym określa się najniższy poziom infrastruktury sieci komputerowych – łącza, urządzenia przesyłające, centrale itp. Więcej na ten temat na internetowej stronie pod adresem: http://en.wikipedia.org/wiki/Backbone_network.

funkcjonowanie państwa w krytycznych sektorach jego działalności. Rozszerzenie to chociaż, że nie wyjaśnia wprost charakteru samych „powiązań internetowych" (logiczne/fizyczne), to jednoznacznie wskazuje iż elementami cyberprzestrzeni są również elementy tworzącej jej infrastruktury teleinformatycznej. Definicja „cyberprzestrzeni RP" uzupełnia ponadto definicję „cyberprzestrzeni" o inny istotny element: możliwości oddziaływania na siebie cyberprzestrzeni oraz „fizycznej" rzeczywistości – w ujęciu potencjalnych zagrożeń, które płyną z ewentualnego zaburzenia funkcjonowania systemów wspierających funkcjonowanie infrastruktury krytycznej. Kwestia ta, zupełnie pominięta na gruncie definicji cyberprzestrzeni mającej mieć charakter wyjściowy, stanowiła również istotny element w przybliżonej wcześniej strategii holenderskiej[146]. Żadna z przytoczonych powyżej krajowych definicji nie wprowadza natomiast relacji z użytkownikami, w zupełności pomijając ten obszar.

Komentarza wymaga w tym miejscu również samo wprowadzenie do ujęcia polskiego idei wydzielenia cyberprzestrzeni krajowej. Koncepcja ta, znana z rozwiązań amerykańskich[147], opiera się na założeniu, że z globalnej cyberprzestrzeni, tworzonej przez systemy teleinformatyczne rozsiane po całym świecie - a więc pozostające pod jurysdykcją różnych państw, możliwe jest wydzielenie takiej jej części, w której tylko jedno państwo ma prawo pełnić suwerenną władzę. Jak zostało zauważone już wcześniej, przy okazji prezentacji amerykańskiej Narodowej Strategii dla Bezpiecznej Cyberprzestrzeni, koncepcja ta pozostaje aktualnie zupełnie nieefektywna z uwagi na brak jakichkolwiek kryteriów, które pozwalałyby na wydzielenie z ogólnoświatowej cyberprzestrzeni, tylko tych zasobów, których zarząd pozostaje w gestii jednego rządu. Niemożliwość ta wynika z istoty budowy rozległych sieci teleinformatycznych, dla których podstawą jest rozszerzalność oraz interoperacyjność stosowanych rozwiązań. Pojęcia te odnoszą się do budowania technologii o zasięgu globalnym, funkcjonujących w oparciu o ściśle współpracującą ze sobą infrastrukturę rozlokowaną po całym globie. Dla prostego zobrazowania zagadnienia - nawet z pozoru proste otwarcie strony internetowej przy użyciu przeglądarki WWW może wiązać się z transferowaniem naszego ruchu sieciowego przez łącza wielu krajów, zbudowane oraz serwisowane przez podmioty podległe właściwości wielu, często bardzo zróżnicowanych, systemów prawnych.

Realne wydzielenie krajowej cyberprzestrzeni możliwe byłoby wyłącznie poprzez fizyczne odseparowanie systemów teleinformatycznych danego państwa od sieci globalnej, co oznaczałoby w istocie tworzenie wielu, zupełnie niezależnych od siebie (a więc przede

[146] Krajowa Strategia Cyberbezpieczeństwa. Sukces poprzez współpracę.
[147] Narodowa Strategia dla Bezpiecznej Cyberprzestrzeni.

wszystkim niewspółdzielących zasobów) „krajowych cyberprzestrzeni". Należy jednocześnie zaznaczyć, że z konieczności logicznej, próba wydzielenia jednej cyberprzestrzeni państwowej oznacza w istocie próbę rozparcelowania całej cyberprzestrzeni pomiędzy poszczególne kraje. Występująca tu nieefektywność stosowania typowych geograficznych kryteriów podziału, potwierdza jednak konieczność badania cyberprzestrzeni pod kątem jej specyfiki oraz stanowi jeden z najważniejszych argumentów przemawiających za uznaniem na arenie międzynarodowej faktycznego wykreowania tej nowej ponad-krajowej (w rozumieniu terytorialnym) domeny i wytworzeniem dla niej nowych zasad prawnych.

Przedstawione powyżej niedostatki pierwszej krajowej definicji cyberprzestrzeni stały się w niedługim czasie powodem dla podjęcia prób jej przemodelowania w ramach prac nad kolejną, następczą po latach 2009 - 2011, wersją programu ochrony cyberprzestrzeni. Jego druga edycja przygotowywana była wstępnie, jako dokument programowy na lata 2011 – 2016, choć ostatecznie została wprowadzona w życie w formie dokumentu bezterminowego z uwagi na przedłużające się prace legislacyjne[148]. Odnosząc się zatem do samego projektu Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011 - 2016, należy zaznaczyć, iż bez zmian w stosunku do wersji poprzedniej pozostawiono samą koncepcję wydzielenia krajowej części cyberprzestrzeni, również w tym przypadku nazywanej cyberprzestrzenią RP, choć same definicje omawianych pojęć uległy istotnej przebudowie. Ich nowe wersje, opierając się na pierwszych doświadczeniach praktycznych, przyjęły następujące brzmienie:

> „Cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami."[149].
>
> „Cyberprzestrzeń RP (dalej jako CRP) – cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)."[150].

Analizując zmiany, jakie zaszły w obu definicjach, w pierwszej kolejności zauważyć należy, że ich nowe ukształtowanie zostało pozbawione bezpośredniego odniesienia do Internetu, jako podstawowej sieci o zasięgu globalnym. Rozszerzono tym samym obszar cyberprzestrzeni także na sieci lokalne, zarówno te połączone, jak i oddzielone od sieci WWW, co nie stoi jednak na przeszkodzie przyjęciu twierdzenia, że w dalszym ciągu

---

[148] Projekt pierwotnie funkcjonował pod tytułem „Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016", by jednak w czasie wydłużających się prac legislacyjnych zostać przemianowanym na „Politykę ochrony cyberprzestrzeni".

[149] Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, s. 6. Tekst dostępny na stronie internetowej pod adresem: http://bip.mswia.gov.pl/portal/bip/6/19057.

[150] Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, s. 6.

głównym składnikiem tak definiowanej cyberprzestrzeni jest Internet. Jednocześnie definicje uległy rozbudowie oraz rozszerzeniu zakresowemu poprzez uzupełnienie ich o nowe, niewymienione we wcześniejszej iteracji, składniki cyberprzestrzeni.

Brak odwołania do Internetu zastąpiono tu nową konstrukcją „cyfrowej przestrzeni przetwarzania oraz wymiany informacji". Usunięto tym samym pojęcie „przestrzeni komunikacyjnej", zastosowane w definicji pochodzącej z programu na lata 2009 – 2011, by w zamian zaproponować dookreślenie przestrzeni jako „cyfrowej". Należy ocenić, że zabieg ten miał za zadanie podkreślić nieobserwowalność przy wyłącznym użyciu ludzkich zmysłów, zjawisk zachodzących w cyberprzestrzeni. By przedstawić to zagadnienie bardziej obrazowo – zgodnie z omawianą cechą, informacje zaczynają podróżować w osobliwym obszarze cyberprzestrzeni dopiero w momencie uzyskania cyfrowej postaci, a tym samym np. ludzki głos wypowiadany w stronę komputera z zainstalowanym komunikatorem głosowym jeszcze nie jest elementem wspomnianej cyfrowej wymiany, zaś staje się nim w momencie przechwycenia za pomocą mikrofonu, przetworzenia przez sterowane odpowiednim oprogramowaniem komponenty sprzętowe komputera oraz „wprowadzeniu" naszej wypowiedzi jako informatyczny zapis na nośnik danych lub do sieci w postaci tzw. pakietów.

Osobnego podkreślenia wymaga także zastosowanie w analizowanej definicji wyrażenia „przetwarzanie oraz wymiana informacji", którego zakres znaczeniowy jest zdecydowanie szerszy od zastosowanego w poprzednim programie rządowym „komunikowania". Przetwarzanie obejmuje bowiem także operacje niepolegające na przekazywaniu informacji, jak np. samo ich wytwarzanie, czy modyfikowanie. Tym samym, na gruncie przywołanej definicji, działania dokonywane w systemach nie muszą polegać na wymianie danych, by móc i tak zakwalifikować je do działań w cyberprzestrzeni. Wątpliwości w tym miejscu budzi jednak ustalenie, czy system odseparowany fizycznie od jakiejkolwiek infrastruktury, a więc z natury rzeczy niemogący w ogóle dokonywać wymiany danych, może być uznany za element cyberprzestrzeni. Stosując wykładnię językową należałoby opowiedzieć się za udzieleniem odpowiedzi negatywnej na tak postawione pytanie, bowiem obie funkcjonalności cyberprzestrzeni – to jest przetwarzanie oraz wymiana danych, połączone zostały spójnikiem „i" ustanawiającym koniunkcję elementów. O ile zatem sama operacja na danych nie musi polegać na ich przesyłaniu, o tyle musi być dokonywana w systemie umożliwiającym wymianę danych, by była uznawana za dokonaną w cyberprzestrzeni. Tym samym, zastosowane zostało tu rozwiązanie analogiczne do znanego

z drugiej strategii Angielskiej[151].

Nowa definicja wskazała również elementy infrastrukturalne budujące cyberprzestrzeń identyfikując je poprzez pojęcia „systemów i sieci teleinformatycznych". Brak określenia znaczenia wskazanych pojęć w samym programie, choćby poprzez odesłanie do innego dokumentu, wymusza jednak poszukiwanie ich znaczenia w innych źródłach prawnych – w szczególności zaś w obowiązujących ustawach oraz wydawanych do nich rozporządzeniach, gdzie terminy te są wykorzystywane. O ile kwestie te zostaną pogłębione dalej, w części rozdziału poświęconej analizie pierwszej ustawowej definicji cyberprzestrzeni (zawartej w noweli ustawy o stanie wojennym oraz niektórych innych ustaw), o tyle w tym miejscu wskazać należy na brak precyzji programu w poruszonym zakresie oraz płynące stąd konsekwencje. Łącznie określeniami „systemy teleinformatyczne" oraz „sieci teleinformatyczne" posługiwała się bowiem ustawa o ochronie informacji niejawnych z 1999 r.[152], która w trakcie prac nad programem została zastąpiona ustawą o tym samym tytule z roku 2011[153]. Późniejszy akt normatywny został pozbawiony pojęcia „sieci teleinformatyczne", zaś zawarta w nim definicja systemów uległa zmianie oraz została zbudowana w oparciu o przepisy innego aktu, mianowicie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[154]. Tym samym, niejednoznaczne stało się ustalenie, do której ustawy należy odnosić się przy określaniu zbioru desygnatów wykorzystywanego w programie pojęcia „systemy teleinformatyczne", zaś brak w nowym porządku prawnym definicji „sieci teleinformatycznych", spowodował, iż interpretacja legalna tegoż pojęcia stała się możliwa wyłącznie w oparciu o przepisy już nieobowiązujące. Pojawiające się nieścisłości zostały w istocie spowodowane niepotrzebnym pomieszaniem pojęć znanych z dwóch dziedzin prawnych: informatyzacji oraz ochrony informacji niejawnych, podczas gdy w programie wyraźnie zapisano, że jego obszar zadaniowy nie dotyczy w ogóle tej drugiej sfery[155]. Nadmiernie wydłużający się czas opracowania programu stał się natomiast przysłowiowym języczkiem u wagi, przypieczętowując rozziew pomiędzy zapisami programu a warstwą normatywną obowiązujących przepisów.

Wracając jednak do analizowanej definicji cyberprzestrzeni z projektu rządowego programu na lata 2011 - 2016, należy także zwrócić uwagę na jej dwa pozostałe elementy:

[151] Strategia Cyber Bezpieczeństwa Zjednoczonego Królestwa (z 2011 r.).
[152] Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 1999 r. Nr 11, poz. 95 z późn. zm).
[153] Ustawa z dnia 5 sierpnia 2011 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167, z późn. zm).
[154] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565, z późn. zm.).
[155] Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, s. 5.

powiązania pomiędzy elementami infrastrukturalnymi oraz relacje z użytkownikami. Pierwszy z nich wskazuje na spójność środowiska cyberprzestrzeni – budowane jest ono nie tyle przez pojedyncze systemy, czy tworzone przez nie sieci, lecz cały system powiązań oraz połączeń pomiędzy tymi składnikami, które wzajemnie oddziaływują na siebie, co w dużej mierze odbywa się w sposób zautomatyzowany oraz często nie jest uświadamiane przez użytkowników. „Relacje z użytkownikami" wprowadzają zaś do pojęcia cyberprzestrzeni nie tylko sam czynnik ludzki (bez którego ostatecznie cyberprzestrzeń nie byłaby dla nas w ogóle istotna), ale także swojego rodzaju punkt styku pomiędzy przestrzenią cyfrową a *fizycznymi* ludźmi. Będąc użytkownikami cyberprzestrzeni wchodzimy w różnorodne, dwustronne relacje ze wszystkimi jej składnikami: czy to przetwarzając zgromadzone w niej zasoby, wprowadzając dane, dokonując zakupów usług lub towarów, czy wreszcie oddziaływując na innych użytkowników lub nawet otaczającą nas rzeczywistość, która coraz częściej uzależniona jest od poprawnego funkcjonowania systemów teleinformatycznych tworzących cyberprzestrzeń. Wiele z pojawiających się faktycznie relacji ma jednak charakter czysto techniczny (np. zapytania do serwera DNS, bez których ruch sieciowy nie byłby w ogóle możliwy) oraz, zgodnie z wcześniejszą uwagą dotyczącą budowy sieci, pozostaje dla większości użytkowników w zupełnym ukryciu.

Utrzymując koncepcję wydzielenia z cyberprzestrzeni tej jej części, która znajduje się pod jurysdykcją Polski, w rządowym programie Polityki ochrony cyberprzestrzeni dokonano jednak zmiany w sposobie definiowania obszaru, zwanego cyberprzestrzenią RP. Cyberprzestrzeń RP została tym razem zdefiniowana, jako cyberprzestrzeń funkcjonująca w obrębie terytorium państwa Polskiego oraz lokalizacjach poza jego terytorium, gdzie funkcjonują państwowe jednostki organizacyjne. Zakres tego pojęcia uległ zatem rozszerzeniu z dwóch powodów – po pierwsze rozszerzony został zbiór desygnatów samej cyberprzestrzeni, po drugie zaś zasięg geograficzny powiększono o miejsca, które wprawdzie nie znajdują się w granicach państwa polskiego, jednak pozostają w jego zainteresowaniu – np. miejsce stacjonowania wojska polskiego. W tym miejscu za błąd należy uznać przykładowe wskazanie placówek dyplomatycznych jako znajdujących się poza obszarem terytorium RP, gdyż zgodnie z prawem międzynarodowym stanowią one przecież obszar eksterytorialny, włączony do obszaru państwa gościa. Definicja ta, powielając niestety niedostatki wskazane przy okazji analizy definicji cyberprzestrzeni RP pochodzącej z programu na lata 2009 – 2011, zasygnalizowała jednak konieczność odejścia przy określaniu jurysdykcji w cyberprzestrzeni od sztywnego kryterium granic państwowych, zupełnie niewydajnego w przypadku domeny, której międzynarodowość stanowi jedną

z podstawowych cech. Niestety jednak także i w tym przypadku posłużono się odwołaniem do wymiarów geograficznych poprzez konkurencję: obręb terytorium państwa Polskiego oraz obręb poza-terytorium, co *de facto* oznacza uznanie wszech-właściwości, zupełnie nierealne w praktycznym ujęciu współpracy międzynarodowej. Tym samym, wprowadzając pozytywne zmiany do definicji pojęcia cyberprzestrzeni, nie dokonano żadnej realnej poprawy w sposobie identyfikowania krajowych zasobów cyberprzestrzeni wciąż próbując fizycznie dzielić samą nie-fizyczną przestrzeń cyfrową.

Kolejnym etapem budowy krajowej definicji cyberprzestrzeni stało się dosyć nieoczekiwane, zarówno w czasie, jak i sposobie (wykorzystano efekty prac nad nowym, jednak nieprzygotowanym jeszcze projektem kolejnego dokumentu programowego), implementowanie przedmiotowego pojęcia do aktu rangi ustawowej. W dniu 2. listopada 2011 r. w życie weszła bowiem ustawa nowelizująca regulacje stanów nadzwyczajnych (zat. ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw - Dz. U. Nr 222, poz. 1323), która implementując do polskiego porządku prawnego kwestię ochrony cyberprzestrzeni, wprowadziła do niego również definicję omawianego pojęcia. Opierając się jeszcze na projekcie Rządowego programu ochrony cyberprzestrzeni RP na lata 2011-2016, zawarta w noweli definicja cyberprzestrzeni, przyjęła następujące brzmienie:

> „Przez cyberprzestrzeń (…) rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.”[156].

Podkreślenia w tym miejscu wymaga fakt, iż ustawa nie posługuje się pojęciem cyberprzestrzeni RP. Zabieg ten, potwierdzając przedstawione wcześniej mankamenty oraz nieskuteczność tego pojęcia, należy uznać, miał na celu również wyraźne objęcie zakresem ustawy także tych zdarzeń, które występują poza krajową częścią cyberprzestrzeni – określanej zgodnie z definicjami zawartymi w obu wersjach rządowego programu. Zagadnienie to, dla porządku wywodu, przedstawione zostało szerzej na końcu analizy definicji, przy okazji prezentacji kontekstu występowania pojęcia cyberprzestrzeni

[156] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222, poz. 1323).

w znowelizowanych przepisach.

Jedyną różnicą w przedstawionej wyżej definicji cyberprzestrzeni, jaka pojawiła się w stosunku do pierwowzoru z projektu programu RPOC 2011-2016, stało się doprecyzowanie zakresu elementów infrastrukturalnych stanowiących podbudowę cyfrowej domeny. Ponieważ w pozostałym zakresie pełną aktualność zachowują uwagi poczynione powyżej, w tym miejscu szerzej przeanalizowane zostaną wyłącznie konsekwencje płynące z wprowadzenia wskazanej zmiany. I tak, problematyczne pojęcie „systemów oraz sieci teleinformatycznych", którego wady zostały poruszone powyżej, zastąpiono tu jasnym, jednoznacznym odwołaniem do pojęcia „systemów teleinformatycznych" zdefiniowanego w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne[157] – odnośnie której zauważyć należy, że siatka pojęciowa pochodząca z tego aktu normatywnego przybrała ostatnio charakter centralnego punktu odniesienia w dziedzinie polskiego prawa informatycznego[158]. Przyjrzyjmy się zatem definicji systemów teleinformatycznych zawartej w ustawie o informatyzacji:

> „Zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne."[159]

Na potrzeby dalszej analizy, definicję tę należy uzupełnić dodatkowo wywodzącymi się z prawa telekomunikacyjnego definicjami pojęć „sieć telekomunikacyjna" oraz „urządzenie końcowe":

> „Sieć telekomunikacyjna – systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju."[160].
>
> „Telekomunikacyjne urządzenie końcowe – urządzenie telekomunikacyjne

[157] Definicja w tej ustawie wywodzi się z kolei z definicji wpisanej do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1244) oraz poprawia wyłącznie odwołanie do przepisów ustawy – Prawo telekomunikacyjne.

[158] Między innymi również ustawa o ochronie informacji niejawnych z 2011 r. odwołuje się wprost do definicji zawartych w ustawie o informatyzacji […].

[159] Art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565, z późn. zm).

[160] Art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.).

przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci.”[161].

Z powyższego zestawienia definicji wynika, że cyberprzestrzeń – rozumiana na gruncie ustawowym – technologicznie tworzona jest przez zbiór możliwych do wyodrębnienia systemów, które budowane są z urządzeń informatycznych. Ich funkcjonalność, zapewniana przez stosowne oprogramowanie, polega na przetwarzaniu danych, w tym ich przesyłaniu za pośrednictwem wszelkiego rodzaju systemów transmisyjnych. Wymiana danych poprzez sieci może odbywać się zarówno przewodowo, jak i radiowo, jednak niezbędne dla funkcjonowania sieci jest zaopatrzenie jej zakończeń w odpowiednie urządzenia końcowe. Na prostym przykładzie domowego łącza internetowego – sieci będącej w praktyce głównym składnikiem cyberprzestrzeni, zakończeniem sieci jest zwykłe gniazdko telefoniczne lub gniazdko kabla koncentrycznego (używanego w usłudze tzw. stałego łącza, najczęściej świadczonej równolegle z usługami telewizyjnymi). Urządzeniem końcowym w tym przykładzie jest modem, w tym modem z łącznością bezprzewodową. System teleinformatyczny zaś to najczęściej zwykły komputer, zbudowany z szeregu podzespołów, jak: płyta główna oraz zamontowane na niej procesor, karta graficzna czy dysk twardy, zaopatrzony także w niezbędne oprogramowanie - nie tylko to instalowane przez użytkownika, ale także zaimplementowane w poszczególnych komponentach.

Zastosowanie ustawowej definicji systemów teleinformatycznych pozwoliło także jednoznacznie rozstrzygnąć kwestię wątpliwości pojawiających się wcześniej na gruncie projektu rządowego programu na lata 2011 – 2016, dotyczących zaliczania do cyberprzestrzeni systemów, które pozostają fizycznie oddzielone od innych systemów. Systemy odseparowane nie zapewniają bowiem możliwości wymiany danych, stanowiącej jedną z funkcjonalności systemów teleinformatycznych zdefiniowanych w ustawie o informatyzacji […]. W świetle przedstawionego powyżej zestawienia, oznacza to, że systemy takie nie zaliczając się do desygnatów pojęcia „system teleinformatyczny”, nie stanowią w ogóle elementu cyberprzestrzeni.

Analizując zaprezentowany w ustawie sposób definiowania cyberprzestrzeni, nie sposób nie przedstawić także kontekstu, w jakim pojęcie to występuje w znowelizowanych przepisach. Jego wprowadzenie pozwala bowiem nadać omawianemu pojęciu właściwego, praktycznego znaczenia, a co za tym idzie, uzupełnić jego treść. Wprowadzenie pojęcia cyberprzestrzeni do ustaw o stanach nadzwyczajnych dokonane zostało zatem w poniższych konfiguracjach:

[161] Art. 2 pkt 43 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm).

„W razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami o charakterze terrorystycznym lub w cyberprzestrzeni […] Prezydent Rzeczypospolitej Polskiej może, na wniosek Rady Ministrów, wprowadzić stan wojenny na części albo na całym terytorium państwa."[162],

„W sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwałę o skierowaniu do Prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego."[163], oraz

„Katastrofę naturalną lub awarię techniczną mogą wywołać również zdarzenia w cyberprzestrzeni oraz działania o charakterze terrorystycznym."[164].

Powyższe zestawienie fragmentów aktów normatywnych pozwala stwierdzić, że istotne z punktu widzenia polskiego porządku prawnego (a w efekcie rodzące określone konsekwencje prawne) jest zaistnienie w cyberprzestrzeni zagrożenia godzącego w określone dobra prawnie chronione. Źródło ataku, czy zdarzenia – wewnętrzne lub zewnętrzne, ale także jego fizyczny cel, schodzą w tym miejscu niejako na drugi na drugi plan. Prezentowana tu cyberprzestrzeń zachowuje zatem pełną spójność, nie będąc przedmiotem podziału pomiędzy poszczególne państwa. Przyjęte rozwiązanie oznacza w efekcie prawną możliwość reagowania na incydenty sieciowe nie tylko te zamykające się w granicach państwa – a więc takie, gdzie zarówno źródło, jak i jego efekty występują w kraju, ale również te przekraczające granice międzynarodowe. Warunkiem zastosowania określonych środków jest naruszenia wymienionych w ustawie dóbr, które odbyło się poprzez wrogie działania lub zdarzenia, które nastąpiły w cyberprzestrzeni.

Zbierając najistotniejsze cechy definicji cyberprzestrzeni pochodzącej z ustawy o zmianie ustawy o stanie wojennym […] z dnia 30 sierpnia 2011 r.[165], wskazać zatem należy, że definicja ta wprowadziła do krajowego porządku prawnego ideę jednej

[162] Zmiana wprowadzona do art. 2 ust. 1 ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. Nr 156, poz. 1301).

[163] Zmiana wprowadzona do art. 2 ust. 1 ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz. U. Nr 113, poz. 985).

[164] Zmiana wprowadzona do art. 3 ust. 2 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. Nr 62, poz. 558).

[165] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222, poz. 1323).

cyberprzestrzeni, będącej wydzielonym logicznie obszarem - cyfrową domeną przetwarzania oraz wymiany informacji. Przestrzeń ta, mająca charakter ponadnarodowy, tworzona jest przez systemy teleinformatyczne połączone za pośrednictwem sieci telekomunikacyjnych, w tym sieci, których elementy infrastrukturalne zlokalizowane są na terenie innych państw. Działanie w cyberprzestrzeni nie ogranicza się wyłącznie do wymiany informacji, może zaś równie dobrze polegać na samym ich wytwarzaniu, modyfikowaniu, czy po prostu odczytywaniu. Również te operacje są zatem dokonywane na gruncie domeny cyfrowej.

Podkreślić w tym miejscu jednak należy, że systemy, które pozostają odcięte od sieci, a zatem nie mogą w ogóle realizować funkcji wymiany informacji, nie stanowią fizycznego elementu tak zdefiniowanej cyberprzestrzeni, a zatem działanie w nich nie może być kwalifikowane jako działanie w cyberprzestrzeni. Definicja wskazując także na wzajemne relacje systemów z użytkownikami, podkreśla swojego rodzaju dwustronne powiązanie działań w cyberprzestrzeni z działaniami w *fizycznej* rzeczywistości, oraz ich wzajemne konsekwencje.

W niespełna dwa lata od wydania w 2011 r. omawianej wyżej zmiany regulacji stanów nadzwyczajnych, wprowadzona na poziomie ustawy definicja pojęcia „cyberprzestrzeń" została powtórzona także na gruncie nowego rządowego programu ochrony cyberprzestrzeni, który ostatecznie - z uwagi na przeciągające się prace nad programem na lata 2011 - 2016, otrzymał nazwę „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" (2013)[166]. Z uwagi na charakter polityki - stanowiącej dokument rządowy o charakterze programowym, definicja zawarta w uchwalonej przez Radę Ministrów Polityce Ochrony Cyberprzestrzeni zachowała pełną spójność z omawianą wyżej definicją ustawową. W związku z powyższym - definicja ta nie wymaga także dodatkowego omawiania. W tym miejscu podkreślić jedynie należy, iż *de facto* definicja ustawowa wprowadzona nowelą z 2011 r. została wypracowana w ramach prac eksperckich prowadzonych nad projektem Polityki Ochrony Cyberprzestrzeni. Na gruncie wskazanej Polityki zastosowano także analogiczną w stosunku do projektu Rządowego Programu Ochrony Cyberprzestrzeni na lata 2011 - 2016 (pomimo minimalnych zmian semantycznych) definicję „cyberprzestrzeni RP". Z uwagi na odpowiedniość przywoływanych definicji - wcześniejsze uwagi zachowują w tym miejscu pełną aktualność.

[166] Pełny tekst Polityki Ochrony Cyberprzestrzeni RP dostępny na stronie internetowej pod adresem: http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-CyberprzestrzeniRzeczypospolitej-Polskiej.html.

§ 2. Definiowanie przestępczości w cyberprzestrzeni - analiza stosowanych pojęć

Choć wyrażenia takie jak *przestępczość komputerowa*, czy *cyberprzestępczość* nie należą w obowiązującym stanie prawnym do katalogu polskich wyrażeń ustawowych, nie sposób nie zgodzić się z twierdzeniem, że odnoszą się one do jednego z największych zjawisk przestępnych dzisiejszych czasów[167]. Zgodnie z aktualnymi szacunkami, łączna wartość globalnych strat ponoszonych na skutek występowania cyberprzestępstw porównywalna jest nawet do wartości całego rynku narkotykowego, plasując się na poziomie 388 miliardów dolarów rocznie[168]. Jak wynika z przeprowadzonych badań, ofiarami wszelkich form nielegalnej działalności w Internecie (w tym także związanej z rozsiewaniem wirusów komputerowych oraz innych typów oprogramowania złośliwego) pada rocznie omalże pół miliarda ludzi, dając globalną średnią około 14 ofiar tego typu bezprawnej aktywności na sekundę. Przenosząc się na grunt krajowy, według oficjalnych danych Policji[169], w Polsce w 2010 r. zgłoszono prawie 8.000 przestępstw popełnionych w sieci, z czego ponad 6.000 przypadków oszustw. W roku 2012 ogólna liczba przestępstw komputerowych odnotowanych w kraju oscylowała już na poziomie 19.000 (z czego około 3/4 to przypadki oszustw), by w roku 2015 przekroczyć poziom dwudziestu tysięcy. Potęgując zagrożenie, należy zaznaczyć, że ogromna liczba przestępstw komputerowych pozostaje ukryta w szarej strefie, wymykając się wszelkim statystykom[170].

Specyfika przestępstw popełnianych w cyberprzestrzeni powoduje bowiem, że wiele czynów tego typu pozostaje niewykrytych lub wymyka się poprawnej identyfikacji jako przestępstwo. Powodem takiego stanu rzeczy nierzadko staje się wręcz brak *technicznej* świadomości samego użytkownika komputera lub innego urządzenia, o tym, że padł właśnie ofiarą cyberprzestępcy. Z drugiej strony, zdarzenia, które są wykrywane i poprawnie kwalifikowane jako przestępne, nie zawsze też zostają zgłoszone do ścigania. W przypadku dużych firm, zachowanie w tajemnicy informacji o poddaniu się skutecznemu atakowi hackerskiemu, w trakcie którego przełamane zostały zbyt słabe zabezpieczenia infrastruktury teleinformatycznej przedsiębiorstwa, może nie tylko stanowić próbę ochrony swojego wizerunku, ale także sposób na uniknięcie ewentualnych konsekwencji odszkodowawczych (np. informacja o cyberataku na bank, w wyniku którego mogło dojść do wycieku poufnych

---

[167] Tak np. M. Siwicki, Cyberprzestępczość, C. H. Beck, Warszawa 2013, s. 9 i nast.

[168] Dane z raportu Norton Cybercrime Report 2011, dostępnego w wersji elektronicznej na stronie internetowej pod adresem: http://pl.norton.com/cybercrimereport/.

[169] Dane pochodzą z oficjalnej strony internetowej Policji, dostępnej pod adresem: http://www.statystyka.policja.pl/portal/st/840/71787/Przestepstwa_popelniane_w_sieci.html.

[170] M. Kliś, Przestępczość w Internecie. Zagadnienia podstawowe, Czasopismo Prawa Karnego i Nauk Penalnych, Wydawnictwo Polska Akademia Umiejętności, Kraków 2000, opracowanie dostępne na stronie internetowej pod adresem: http://prawo.vagla.pl/node/905.

danych jego klientów).

W świetle przytoczonych wyżej danych, suma zysków, które potencjalnie mogą być generowane przez cyberprzestępczość, czyni ten rodzaj działalności jedną z najbardziej lukratywnych gałęzi przestępczości w ogóle, przyciągając nie tylko drobnych złodziei i oszustów, ale także cybergangi specjalizujące się w nowoczesnych technologiach, czy wreszcie *konwencjonalne* zorganizowane grupy przestępcze, chcące rozszerzyć swój dotychczasowy obszar aktywności. W każdym z tych przypadków, cyberprzestępczość pozostaje działalnością relatywnie tanią, dającą ogromne możliwości (nie tylko finansowe, ale także np. terrorystyczne), a przy tym wciąż uważaną za zapewniającą większe bezpieczeństwo niż inne, tradycyjne formy działalności przestępnej - tak ze strony funkcjonowania wymiaru sprawiedliwości, jak i działań innych, rywalizujących przestępców[171]. Można powiedzieć, że wszelkie słabości cyberprzestrzeni, stają się automatycznie siłą napędową dla nowoczesnych przestępców.

Pomimo, że określenie „cyberprzestępczość"[172], jak i inne wyrażenia stosowane do opisu poruszanego tu fenomenu, wciąż nie stanowią ścisłej kategorii prawnej, precyzyjna rekonstrukcja ich znaczenia stanowi istotną wartość dodaną dla prezentacji analizowanej gałęzi działalności przestępnej, w tym jej zakresu oraz specyfiki[173]. Celem rozważań zawartych w niniejszym rozdziale jest zatem podjęcie próby uporządkowania stosowanych pojęć oraz udzielenie odpowiedzi na podstawowe pytania badawcze: czym w istocie jest cyberprzestępstwo, jakie są jego rodzaje oraz, co odróżnia je od innych kategorii przestępstw[174]? Tak zakreślona problematyka pozostaje w ścisłym związku z kwestią określenia, jakie (jak ujęte?) dobra prawnie chronione stanowią przedmiot zamachu tego

---

[171] G. L. Fortinet, *Fighting Cybercrime: Technical, Juridical and Ethical Challenges*. Opracowanie dostępne na stronie internetowej pod adresem: http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf.

[172] Termin powstał jeszcze w początku lat dziewięćdziesiątych oraz oficjalnie został użyty przez tzw. Grupę z Lyon, działającą w ramach G8, której zadaniem było prowadzenie prac analitycznych nad nowymi formami przestępczości, za: S. Perrin, *Cybercrime* w: A. Ambrosi, V. Peugeot, D. Pimienta, *Word Matters: multicultural perspectives on information societies, C & F Editions, Francja 2005. Opracowanie dostępne w wersji elektronicznej na stronie internetowej pod adresem: http://media.mcgill.ca/en/word_matters. A. Adamski zwraca także uwagę na zastosowanie analizowanego terminu w roku 1996 przez L. E. Quarantiello w: Cyber Crime: How to protect yourself from computer criminals, Wyd. Tiare Pubns. Tak w: A. Adamski, Prawo karne komputerowe, CH Beck, Warszawa 2000, s. 30 i nast.*

[173] Niektórzy autorzy poddają wręcz pod wątpliwość, czy czyny wchodzące w zakres pojęć odnoszących się do cyberprzestępczości zachowują w istocie homogeniczność. Tak np. U. Sieber, Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka, Przegląd Policyjny, Nr 3, Szczytno 1995, s. 6. Przytaczam za: A. Kania, Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni, *e-biuletyn* CBKE 1/2009, Wrocław 2009, s. 8. Tekst opracowania dostępny jest na stronie internetowej pod adresem: http://bibliotekacyfrowa.pl/Content/34350/Oszustwo_komputerowe.pdf.

[174] Uzupełniająco, kwestia stosowania klasycznego dorobku prawa karnego wobec cyberprzestępczości zaznaczana jest w: K. Dobrzeniecki, Prawo a etos cyberprzestrzeni, Wyd. Adam Marszałek, Toruń 2004, s. 61 i nast.

rodzaju działalności przestępnej. Podobnie, jak w przypadku definiowania cyberprzestrzeni, także i te rozważania nie mogą ograniczać się wyłącznie do płaszczyzny prawnej, która bez kontekstu technologicznego pozostaje zawieszona w próżni. Definicja cyberprzestępczości prezentowana oraz rekonstruowana jest w oparciu o szereg rozwiązań przyjętych na gruncie piśmiennictwa, aktów około-prawnych oraz powszechnie obowiązujących przepisów - zarówno krajowych (obcych, jak i polskich), ale także powstałych w ramach inicjatyw międzynarodowych. Uzupełniająco, do rozważań wprowadzone zostają także dodatkowe pojęcia wspomagające opis zjawiska cyberprzestępczości - (cyber)incydent oraz (cyber)atak.

Poszczególne rodzaje cyberprzestępstw oraz cyberataków, a także ich kwalifikacja prawna w oparciu o przepisy obowiązującego w Polsce Kodeksu karnego, przeanalizowane zostaną w rozdziale IV, zawierającym część szczegółową rozważań materialno-karnych. W efekcie przyjętej budowy, pełen obraz tego, czym naprawdę jest przestępczość cyberprzestrzeni wyłania się z łącznego ujęcia obu wymienionych części - to jest ogólnej, definicyjnej i szczególnej, opisującej poszczególne kategorie czynów bezprawnych. Należy także podkreślić, że niniejsza część pracy bazuje na definicji oraz charakterystyce cyberprzestrzeni, zawartych w poprzedzających częściach rozdziału. Części te, stanowiąc komplementarne uzupełnienie dla prowadzonych poniżej rozważań, zapewniają naturalną podstawę teoretyczną dla poprawnego ujęcia (też *umiejscowienia*) przestępczości cyberprzestrzeni.

Brak jednolitych rozwiązań prawnych nakierowanych na zapobieganie oraz zwalczanie nowoczesnych form przestępczości komputerowej - powodowany w dużej mierze niechęcią (lub niezdolnością) państw do wypracowywania jednolitych, wspólnych stanowisk, ale także spóźnionym podjęciem odnośnych inicjatyw legislacyjnych, spowodował wytworzenie wyjątkowo niespójnej oraz niejednorodnej siatki pojęciowej, odnoszącej się do obszaru cyberprzestępczości. Nieco ironicznie, w piśmiennictwie zauważa się wręcz, że stosowane w przedmiotowym zakresie pojęcia, mają nierzadko charakter bardziej publicystyczny, niż naukowy[175]. Pogląd ten zasługuje na przyznanie mu racji. Na gruncie dostępnych materiałów, tym samym wyrażeniom często nadawane są także różne, krzyżujące się zakresowo znaczenia. Definicje nierzadko tworzone są *ad hoc* przy okazji tworzenia nowego dokumentu lub opracowania. Na domiar złego, ustawiczne zmiany w obszarze nowoczesnych technologii - stanowiących przecież fundament dla cyberprzestrzeni oraz nowoczesnych usług świadczonych za pośrednictwem sieci komputerowych - również nie

[175] Tak np. A. Adamski, Prawo karne komputerowe, CH Beck, Warszawa 2000, s. 30.

sprzyjają pewności oraz stabilności budowanych definicji[176]. Zasadnym jest zatem, aby podjąć próbę uporządkowania panującego stanu rzeczy.

Poniżej zaprezentowane zostały podstawowe pojęcia, które do tej pory wykorzystywane były do określania nowej kategorii przestępczości *występującej w cyberprzestrzeni*. Do pojęć tych zaliczyć należy, przybliżone kolejno: nadużycie komputerowe, przestępstwo związane z komputerem, bezprawne użycie komputera, przestępstwo komputerowe, przestępstwo powiązane z technologią informacyjną oraz ostatecznie - cyberprzestępstwo. Zaproponowany przegląd definicji oraz kontekstów występowania przywołanych wyrażeń zbudowany został w postaci *quasi*-słownikowej, to jest w podziale na pojęcia. Dla uporządkowania chronologicznego wybranych dokumentów źródłowych oraz ustalenia panujących trendów rozwoju siatki terminologicznej, w końcowej części rozdziału przedstawiona została także tabela porównawcza, zestawiająca w ujęciu czasowym wykorzystane dokumenty oraz zastosowane na ich gruncie pojęcia.

1. Pojęcie „nadużycia komputerowego".

W ujęciu historycznym, proces formułowania nowych, specyficznych pojęć odnoszących się do *przestępczości komputerowej* rozpoczął się jeszcze w połowie lat siedemdziesiątych ubiegłego stulecia. Czasy te były świadkiem pierwszych głośnych, medialnych doniesień o atakach *hackerskich*, które uświadomiły nie tylko szerszej opinii publicznej, ale także przedstawicielom władz rządowych, fakt pojawienia się nowych *cyber* zagrożeń. Warto dodać - zagrożeń, które mogą powodować, jak najbardziej realne straty finansowe. W latach siedemdziesiątych spopularyzowało się także określenie *hacker,* które swoją negatywną konotację otrzymało jednak dopiero w połowie następnego dziesięciolecia[177].

Jednym z pierwszych, szeroko rozpoznawanych opracowań, poświęconych zagadnieniom zwalczania nowoczesnych form przestępczości, stała się wydana w 1976 r. książka autorstwa D. Parkera, zatytułowana „Przestępstwo z wykorzystaniem komputera"[178]. Pomimo swojego tytułu, książka skupiała się jednak wokół pojęcia „nadużycia komputerowego"[179], które definiowane było przez jej autora jako:

„[...] każdy incydent polegający na zamierzonym zachowaniu, którego ofiara poniosła

[176] Trudnościom w budowaniu odnośnych definicji poświęcona była nawet odrębna część Zalecenia Nr R(89)9 Komitetu Ministrów Rady Europy z 1989 r. w sprawie przestępczości komputerowej.
[177] Słowo *hacker* oznaczało pierwotnie (pozytywnie) osobę o wysokich kwalifikacjach komputerowych, potrafiącą w szerokim zakresie wykorzystywać możliwości nowych technologii informatycznych.
[178] D. B. Parker, *Crime by Computer*, Scribner, Nowy Jork, 1976. Tłumaczenie tytułu własne.
[179] W oryginale *„computer abuse"*.

lub mogła ponieść szkodę, zaś sprawca odniósł lub mógł odnieść zysk, wiążący się z komputerami.”[180].

Uzupełniająco, opracowanie wskazywało także cztery role, w jakich występować może komputer w tak określonym nadużyciu:

1) komputer lub zgromadzone na nim dane, jako przedmiot ataku;
2) komputer, jako narzędzie wytwarzające specyficzne środowisko lub nowe formy dóbr prawnych podlegających ochronie;
3) komputer, jako środek lub narzędzie służące do popełnienia nadużycia; oraz,
4) komputer, jako symbol użyty dla zastraszenia lub oszustwa[181].

Choć wskazane role częściowo przeplatały się zakresowo, każda z nich odnosiła się do specyficznego aspektu dokonywania nadużyć komputerowych. Pierwsza, nawiązywała do ochrony samych systemów teleinformatycznych oraz przechowywanych na nich danych w postaci elektronicznej, które mogą stać się celem działania przestępnego. Druga, choć zdecydowanie wyprzedzająca swoje czasy, nawiązywała do nowego sposobu postrzegania dóbr prawnie chronionych, które wraz z rozwojem cyberprzestrzeni mogą wyrażać się w zupełnie nowych, nieznanych dotąd formach, wykraczając poza postać typowych praw, ruchomości, nieruchomości oraz dóbr osobistych. Trzecią z ról odnieść można do kategorii nadużyć komputerowych *sensu stricte*, gdzie komputer staje się niezbędnym narzędziem do popełnienia przestępstwa (które może być skierowane także przeciwko nowym dobrom prawnym, na które wskazywano w punkcie 2), zaś czwarta, odwoływała się *de facto* do tych czynów, dla których komputer staje się wyłącznie środkiem komunikacyjnym, zaś samo zachowanie kwalifikować można jako przejaw klasycznych form czynów bezprawnych, jak np. oszustwo, czy zniesławienie.

Pomimo tak szerokiego ujęcia, żadna z wymienionych ról nie odnosiła się jednak bezpośrednio do wykorzystywania komputerów, jako samodzielnego źródła dowodowego, które dostarczać może dowodów także w sprawach nie zaliczających się ściśle do kategorii nadużyć komputerowych. Z uwagi na czasy, w których definicja była budowana - poprzedzające jeszcze powstanie Internetu, żaden z ujętych aspektów nie odwoływał się także specyficznie do kwestii wykorzystania komputera do przeprowadzania ataków za pośrednictwem sieci.

---

[180] A. Reyes, *Cyber Crime Investigations*, Elsevier, USA, 2007, s. 25. W oryginale *„any incident involving an intentional act where a victim suffered or could have suffered a loss, and a perpetrator made or could have made a gain and is associated with computers”*. Tłumaczenie własne.

[181] *Ibidem*, s. 25.

Przytoczona wyżej definicja proponowała, aby dwiema głównymi cechami nadużycia komputerowego były jego umyślność oraz skorelowane (mogące zaistnieć choćby potencjalnie) strata oraz korzyść majątkowa, powstające na wskutek przestępstwa odpowiednio po stronie ofiary oraz napastnika. Innymi słowy, na gruncie definicji, nadużyciem komputerowym nie mógł stać się ani czyn niezamierzony - jak np. nieumyślne uszkodzenie zasobów chronionych, ani taki, który w ogóle nie zakładał możliwości odniesienia korzyści przez jego sprawcę - jak akt wandalizmu polegający na skasowaniu lub podmianie plików strony internetowej. Oba wskazane wymogi, stanowiące przejaw utożsamiania nadużyć komputerowych z przestępczością nastawioną na określone korzyści majątkowe, wiązać należy z dawnym rozumieniem przestępczości komputerowej, jako przestępczości wysoce specjalistycznej, wymagającej świadomego podejmowania skomplikowanych operacji.

Pojęciem „nadużycia komputerowego” posługiwał się następnie, nieco późniejszy - wydany w 1986 r., raport Organizacji Rozwoju i Współpracy Gospodarczej (OECD), zatytułowany „Przestępstwa związane z komputerem: analiza polityki legislacyjnej”[182]. Na łamach raportu, czyn „nadużycia komputerowego” zdefiniowany został roboczo, jako:

> „Każde zachowanie niezgodne z prawem, nieetyczne lub nieuprawnione, odnoszące się do automatycznego przetwarzania oraz przekazywania danych”[183].

Przytoczoną definicję podzielić można na dwie części. Pierwszą - charakteryzującą samo pojęcie nadużycia, oraz drugą - wyznaczającą specyficzny obszar przedmiotowy, w którym popełnione nadużycie, staje się właśnie nadużyciem komputerowym. W zakresie pierwszego elementu, definicja wskazywała trzy następujące kategorie zachowań:

1) działania niezgodne z prawem, a więc wyraźnie zakazane przez przepisy odrębne (w stosunku do administracji publicznej kategorię tę należałoby rozszerzyć także o działania podjęte bez wyraźnej podstawy prawnej);
2) działania nieuprawnione (*nieautoryzowane*) - które rozumieć należy, jako wykonywane bez stosownej zgody osoby uprawnionej do zarządzania systemem, informacją, czy danymi. Działania takie mogą (ale nie muszą) być penalizowane, powodując częściowe krzyżowanie się zakresów kategorii pierwszej oraz drugiej; oraz
3) działania nieetyczne - a więc działania niełamiące żadnych formalnie obowiązujących zasad, lecz sprzeciwiające się szeroko rozumianym zasadom współżycia społecznego.

[182] *Computer-related crime: Analysis of legal policy*, OECD, Paryż 1986.
[183] W oryginale: „*Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data.*”. Tłumaczenie własne.

Wprowadzenie do definicji nadużycia komputerowego kategorii działań nieuprawnionych oraz działań nieetycznych, spowodowało, że pojęcie to - na gruncie raportu OECD, utraciło swoją wyłącznie karnistyczną konotację. Jednocześnie, nabrało cech wyrażenia uniwersalnego, które tak jak pojęcia błędu, czy groźby, mogło być stosowane zarówno w kontekście spraw karnych, jak i tych należących do innych gałęzi prawa. Pomimo przyjętej konstrukcji definicji, raport nie odnosił się jednak w przedstawionym dalej katalogu nadużyć komputerowych do czynów innych, niż należące do kategorii działań niezgodnych z prawem. Szerokiej krytyce poddane zostało natomiast definiowanie nadużycia komputerowego poprzez kategorię działań nieetycznych, która z natury rzeczy pozostaje wysoce nieostra oraz niesformalizowana.

Nie posiada także w całości wymiaru ogólnoświatowego, co ma szczególne znaczenie w dzisiejszych czasach globalnych sieci. Ostatecznie, dodać należy także, że pojęcie działań etycznych w przypadku poruszania się po sieciach komputerowych może miejscami nabierać specyficznego znaczenia z uwagi na zautomatyzowany, elektroniczny charakter wykonywanych operacji - np. nie jest działaniem nieetycznym wywoływanie serwerów podłączonych do sieci, lecz staje się ono wręcz przestępstwem o ile wykonywane jest wielokrotnie w krótkim czasie powodując zawieszenie poprawnego działania usługi (tzw. atak odmowy dostępu - opisany szczegółowo w dalszej części pracy). Podobnie, dyskusyjna może być kwestia oceny etyczności zachowania polegającego na skanowaniu zabezpieczeń stosowanych na stronach internetowych - co z jednej strony może stanowić przygotowanie do ataku, czy szantażu, a z drugiej - służyć oferowaniu usług polegających na poprawie bezpieczeństwa systemów sieciowych. Kwestie tego typu pozostają wciąż nierozstrzygnięte pomimo wieloletniej obecności na forum społeczeństwa internetowego.

W ramach drugiego wyróżnionego elementu - czyli obszaru, w którym popełniane są nadużycia komputerowe, definicja wskazywała na domenę „automatycznego przetwarzania oraz przekazywania danych”. Wyrażenie to, odnosząc się wprost nie tyle do samych danych, co procesów ich przetwarzania (a w tym przekazywania), w istocie obejmowało także ukryte pod tymi procesami systemy teleinformatyczne oraz elementy infrastruktury sieciowej, które choć nie zostały wymienione w definicji wprost - uznać należy za element niezbędny dla ukonstytuowania procesu automatycznego przetwarzania danych. Wyraźne wprowadzenie do definicji elementu przekazywania danych odczytywać należy na tle niezwykle dynamicznego w latach osiemdziesiątych rozwoju sieci, w szczególności zaś Internetu - jako wyraz świadomości, że konieczne jest podejmowanie działań nakierowanych na walkę z zupełnie nowymi zagrożeniami dla danych komputerowych. Tym samym, inaczej niż w przypadku

definicji analizowanego pojęcia, przyjętej na gruncie amerykańskiego opracowania z 1976 r., nadużycie komputerowe wyraźnie odniesiono także do działań wykonywanych za pośrednictwem nowoczesnych sieci teleinformatycznych.

Obok przytoczonej wyżej definicji nadużycia komputerowego, raport OECD określał także enumeratywnie pięć kategorii nadużyć komputerowych, które powinny być penalizowane we wszystkich porządkach prawnych. Zaliczono do nich: oszustwo komputerowe (nastawione na uzyskiwanie korzyści majątkowych), fałszerstwo komputerowe, zakłócenie poprawnego funkcjonowania systemu (sabotaż), nielegalne kopiowanie programów komputerowych oraz nielegalny dostęp do systemu komputerowego uzyskany poprzez naruszenie zabezpieczeń lub w celu wyrządzenia szkody[184].

Katalog typowych nadużyć komputerowych przedstawiony został zatem wyłącznie w kontekście czynów, które powinny podlegać kwalifikacji karnej - w odróżnieniu od podejścia, które zaprezentowano w ramach budowy definicji nadużycia komputerowego. Jednocześnie, przygotowany katalog łączył kategorie ściśle karnistyczne (fałszerstwo, włamanie) z ochroną praw autorskich, nazywając *nadużyciem komputerowym* także kopiowanie programów (dziś zwane potocznie *piractwem komputerowym*), które może być dokonywane w ogóle z pominięciem komputerów. Na marginesie, warto zaznaczyć, że obok analizowanego tu pojęcia, raport OECD posługiwał się również kategorią *przestępstwa związanego z komputerem*, które choć pełniło tu rolę drugorzędną, pojawiało się - dosyć niekonsekwentnie, w samym tytule dokumentu.

Równolegle do wydania raportu OECD, rok 1986 stał się świadkiem także innego doniosłego zastosowania pojęcia „nadużycie komputerowe”, związanego z wydaniem obszernej, amerykańskiej kodyfikacji prawa nastawionej na kompleksowe zwalczanie zagrożeń komputerowych. Wskazana kodyfikacja przybrała formę ustawy zatytułowanej w oryginale *Computer Fraud and Abuse Act*[185], której przepisy stały się podstawowym narzędziem amerykańskiego wymiaru sprawiedliwości w walce z szeregiem przestępstw popełnianych z wykorzystaniem komputera.

Co istotne, pomimo historycznej już daty wprowadzenia ustawy, pozostaje ona aktem wciąż obowiązującym, co nadaje prowadzonym w tym miejscu rozważaniom waloru aktualności. Od chwili wejścia w życie, ustawa była oczywiście wielokrotnie nowelizowana, m. in. w latach 1989, 1994, 1996, 2001 (wydaną po zamachu na WTC ustawą *PATRIOT*

---

[184] A. Adamski, Prawo karne..., op. cit., s. 6.

[185] W tłumaczeniu: Ustawa o komputerowym oszustwie oraz nadużyciu. Tłumaczenie własne. Tekst ustawy dostępny na stronie internetowej pod adresem: http://www.law.cornell.edu/uscode/text/18/1030.

Act[186]) oraz 2008 (ustawą *Identity Theft Enforcement and Restitution Act*[187])[188]. Przepisy wprowadzone przywoływaną ustawą z 1986 r. uzupełniły także stworzoną w 1984 r. sekcję 1030, 47. rozdziału, 18. tytułu amerykańskiego *United States Code*[189], w której to sekcji pierwotnie uregulowana była pokrótce penalizacja szczególnych przypadków uzyskania bezprawnego dostępu do informacji rządowych - przede wszystkim informacji niejawnych oraz informacji finansowych, w sytuacji, gdy informacje te przetwarzane były w komputerach należących do agend rządowych[190]. Sama sekcja 1030 zatytułowana została „Oszustwo oraz podobna działalność w powiązaniu z komputerami"[191].

Ustawą *Computer Fraud and Abuse Act* wprowadzono penalizację szeregu stypizowanych czynów, które - zgodnie z samą nazwą aktu normatywnego, określone zostały łącznie mianem „nadużyć oraz oszustw komputerowych". W odniesieniu do zastosowanej tu nazwy zbiorczej, już na pierwszy rzut oka uwagę zwraca wyraźne wydzielenie oszustwa komputerowego od pozostałych nadużyć komputerowych, co z jednej strony podkreślać może szczególny charakter tego czynu (obejmujący połączenie działań komputerowych z elementami socjotechniki oraz nastawienie na uzyskanie korzyści majątkowej), z drugiej zaś - czyni zasadnym pytanie, czy w tej sytuacji „oszustwo komputerowe" należy na gruncie analizowanego aktu zaliczać do ogólnej kategorii „nadużyć komputerowych"? Wyraźne usytuowanie „oszustw" obok „nadużyć" sugerować mogłoby intencjonalne oddzielenie obu kategorii, przesądzające, że oszustwo nie należy do katalogu nadużyć komputerowych, choć brak jest możliwości potwierdzenia takiej tezy na gruncie samych przepisów. Z uwagi na fakt pozostawienia w treści ustawy wskazanych wyrażeń bez jakichkolwiek definicji, także rekonstrukcja ich znaczenia możliwa jest wyłącznie poprzez prezentację typologii przestępstw ujętych w przepisach aktu. Z uwagi na normatywny charakter analizowanego dokumentu,

---

186 Pisana wielkimi literami nazwa ustawy "*PATRIOT Act*" stanowi skrót od wyrazów: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*. W tłumaczeniu: Jednocząc oraz wzmacniając Amerykę poprzez dostarczenie stosownych narzędzi wymaganych do wykrywania oraz zapobiegania terroryzmowi. Tłumaczenie własne.

187 W tłumaczeniu: Ustawa o ściganiu przestępstwa kradzieży tożsamości oraz jej restytucji. Tłumaczenie własne.

188 C. Doyle, Cybercrime: *An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, Congressional Research Service, s. 1. Tekst pełnego opracowania dostępny na stronie internetowej pod adresem: http://www.fas.org/sgp/crs/misc/97-1025.pdf.

189 *United States Code* (U.S.C.) stanowi swoisty odpowiednik Dziennika Ustaw, który obejmujące skodyfikowane prawo federalne USA. Więcej na temat U.S.C. na stronie internetowej pod adresem: http://en.wikipedia.org/
wiki/United_States_Code.

190 H. M. Jarrett, M. W. Bailie, E. Hagen, S. Eltringham, *Prosecuting Computer Crimes*, *Office of Legal Education Executive Office for United States Attorneys* - wydawnictwo Ministerstwa Sprawiedliwości USA (*Department of Justice*),Washington DC 2010, s. 1. Opracowanie dostępne na stronie internetowej pod adresem: http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

191 W oryginale: „*Fraud and related activity in connection with computers*". Tłumaczenie własne.

forma w jakiej określone zostały kolejne przestępstwa przyjęła typowo kodeksową budowę (np. „kto uzyskuje bezprawny dostęp...”). W efekcie, w przepisach pominięte zostały jakiekolwiek dodatkowe określenia, które miałyby stać się nazwami dla poszczególnych przestępstw. Stosowane w dalszej części analizy, pomocniczo, nazwy rodzajowe, nie pochodzą zatem z samej ustawy, zaś z oficjalnego opracowania Kongresu USA, przynależąc tym samym do sfery języka prawniczego - to jest języka II stopnia.

Amerykańska ustawa „o nadużyciach oraz oszustwach komputerowych” określiła siedem następujących kategorii czynów zabronionych:

1) świadome uzyskanie dostępu do komputera bez uprawnienia lub z przekroczeniem posiadanych uprawnień oraz uzyskanie w ten sposób informacji prawnie chronionych, w tym informacji obronnych lub dotyczących stosunków międzynarodowych, w sytuacji, gdy z okoliczności wynika iż informacje te mogłyby zostać użyte na szkodę USA, a także przekazywanie takich informacji na korzyść jakiegokolwiek państwa obcego;
2) umyślne uzyskanie nieuprawnionego dostępu do komputera bez uprawnienia lub z przekroczeniem posiadanych uprawnień oraz uzyskanie informacji bankowych lub finansowych, informacji przetwarzanych przez organy administracji publicznej lub informacji pochodzących z chronionych komputerów;
3) umyślne uzyskanie nieuprawnionego dostępu do niedostępnego publicznie komputera administracji, który przeznaczony jest do użytku wyłącznie na rzecz rządu USA lub jest używany przez rząd USA, zaś działanie sprawcy wpływa na ten użytek;
4) świadome oraz z zamiarem dokonania oszustwa uzyskanie dostępu do chronionego komputera bez uprawnienia lub z przekroczeniem uprawnień oraz uzyskanie w ten sposób jakiejkolwiek korzyści majątkowej, chyba, że przedmiotem oszustwa oraz jedyną uzyskaną korzyścią jest samo użycie komputera, zaś wartość tego użycia nie przekracza 5.000 dolarów w okresie jednego roku;
5) umyślne spowodowanie szkód w chronionym komputerze poprzez świadome spowodowanie transmisji programu, informacji, kodu lub polecenia, a także uzyskanie dostępu bez uprawnienia;
6) świadoma oraz z zamiarem dokonania oszustwa, nielegalna sprzedaż haseł lub podobnych informacji mogących służyć do uzyskania dostępu do komputera bez uprawnień, pod warunkiem, że takie działanie może wpłynąć na obrót międzystanowy lub zagraniczny, lub dany komputer wykorzystywany jest przez lub na rzecz rządu USA;

7) transmitowanie w ramach obrotu międzystanowego lub zagranicznego jakichkolwiek komunikatów zawierających groźby spowodowania uszkodzeń chronionego komputera, groźby nieuprawnionego uzyskania informacji pochodzących z chronionego komputera lub ich uszkodzenia, a także żądania pieniędzy lub innych korzyści majątkowych w związku z uszkodzeniem chronionego komputera - celem bezprawnego uzyskania korzyści majątkowych od jakiejkolwiek osoby[192].

Uzupełniająco, występujący w przytoczonych hipotezach „chroniony komputer" został zdefiniowany w ustawie federalnej, jako komputer:

„(A) przeznaczony do wyłącznego użytku przez instytucję finansową lub rząd USA, lub w przypadku komputera nie przeznaczonego do takiego wyłącznego użytku, komputer faktycznie używany przez lub dla instytucji finansowej lub rządu USA, którego użytkowanie jest dotykane przez czyn bezprawny; lub

"(B) który jest użytkowany w lub wpływa na międzystanowy lub zagraniczny obrót lub komunikację, włączając komputery zlokalizowane poza terytorium USA, które są użytkowane w sposób wpływający na międzystanowy lub zagraniczny obrót lub komunikację USA;" [193].

Zgodnie z przywołanym wcześniej opracowaniem ustawy sporządzonym na potrzeby Kongresu USA, wyliczone w pkt 1 - 7 przestępstwa można skonstatować rodzajowo, jako odpowiednio: 1) szpiegostwo komputerowe; 2) bezprawne wtargnięcie komputerowe do określonych zasobów rządowych, bankowych, finansowych lub innych przechowywanych na komputerze; 3) bezprawne wtargnięcie komputerowe do zasobów komputera rządowego; 4) oszustwo, którego integralną częścią jest uzyskanie nieuprawnionego dostępu do komputera chronionego, przetwarzającego dane wrażliwe - rządowe, bankowe, lub inne, istotne dla obrotu gospodarczego; 5) uszkadzanie zasobów komputerów chronionych; 6) nielegalny handel hasłami dostępu; oraz 7) groźba uszkodzenia zasobów komputerów chronionych[194]. Na tle skróconego ujęcia wyraźnie rysuje się zasadniczy cel wydania amerykańskiej ustawy - wzmocnienie ochrony systemów rządowych oraz tych wykorzystywanych na potrzeby lub w interesie USA.

Zawarty w ustawie katalog „nadużyć oraz oszustw komputerowych" pozwala także na wyróżnienie czterech podstawowych metod działań właściwych dla regulowanych form przestępczości:

---

[192] Ustawa federalna *Computer fraud and abuse act* (18 U.S.C. 1030), lit. a, pkt 1 - 7. Tłumaczenie własne.
[193] Ustawa federalna *Computer fraud and abuse act* (18 U.S.C. 1030), lit. e, pkt 2. Tłumaczenie własne.
[194] Tak: C. Doyle, *Cybercrime...*, op. cit, część *Summary*.

- w pkt 1 - 4 jest to bezprawne uzyskanie dostępu do komputera, funkcjonalnie połączone z możliwością odczytania przetwarzanych na komputerze danych, zaburzeniem pracy systemu lub bezprawnym wprowadzeniem zmian w danych - zwane w tym ostatnim przypadku oszustwem komputerowym (pkt 4),
- w pkt 5 - wywołanie transmisji danych chronionych prawem (inaczej kradzież danych lub ich bezprawne przesłanie dalej),
- w pkt 6 - sprzedaż haseł oraz innych narzędzi mogących służyć popełnianiu nowoczesnych form przestępczości (bez względu na źródło ich pochodzenia), oraz
- w pkt 7 - grożenie możliwością przeprowadzenia ataku w cyberprzestrzeni.

Warto podkreślić, że żadna z określonych w ustawie kategorii nie odnosi się bezpośrednio do oszustwa komputerowego, jako samodzielnego narzędzia dla uzyskania dostępu do systemu, np. w sytuacji wyłudzenia hasła, które może zostać przeprowadzone nawet poza cyberprzestrzenią (jak choćby telefonicznie, po podszyciu się pod reprezentanta pionu wsparcia teleinformatycznego). Tym samym, na gruncie analizowanych przepisów, dla dokonania oszustwa komputerowego niezbędne jest bezpośrednie działanie sprawcy w cyberprzestrzeni, które nakierowane jest na sfałszowanie przetwarzanych danych w sposób zapewniający uzyskanie określonych korzyści majątkowych.

2. Pojęcie „przestępstwa związanego z komputerem".

Trzy lata po przygotowaniu przez Donna Parkera pierwszego dużego, naukowego opracowania traktującego o fenomenie przestępczości komputerowej - a więc jeszcze w końcówce lat siedemdziesiątych, problematyka zwalczania *cyber*-zagrożeń wprowadzona została na grunt dokumentów rządowych. Pierwszym na świecie *quasi*-normatywnym aktem z zakresu zwalczania tego typu działalności przestępnej, stał się bowiem wydany w 1979 r. podręcznik dla pracowników amerykańskiego wymiaru sprawiedliwości, zatytułowany w oryginale „*Computer Crime: Criminal Justice Resource Manual*"[195]. Rządowy podręcznik, mający stać się ogólną instrukcją postępowania śledczych w sprawach przestępczości dotykającej nowoczesnych technologii, przygotowany został na zamówienie Ministerstwa Sprawiedliwości USA (*Department of Justice*) we współpracy z Instytutem Naukowym Stanforda. Z uwagi na swoje wcześniejsze zaangażowanie w tematyce, udział w pracach brał

[195] *Computer Crime: Criminal Justice Resource Manual, SRI International, National Criminal Justice Information and Statistics Service*, Kalifornia, USA, 1979.

także sam Parker.

Pomimo wcześniejszego dorobku doktryny amerykańskiej, wyrażeniem stosowanym jako centralne na gruncie przywoływanego podręcznika stało się pojęcie „przestępstwa związanego z komputerem”[196] - w oryginale: „*computer-related crime*”. Na marginesie, warto zaznaczyć, że w samym tytule dokumentu, zupełnie niekonsekwentnie posłużono się innym, niezdefiniowanym w podręczniku i wówczas jeszcze stosowanym głównie w kontekście publicystycznym, wyrażeniem „przestępczość komputerowa” (w oryginale „*computer crime*”[197]), zaś w tekście opracowania pojawiały się także inne, również niedefiniowane tu pojęcia, m. in. „nadużycie komputerowe”[198]. Podstawowym określeniem używanym w powoływanym opracowaniu pozostawało jednak „przestępstwo związane z komputerem”, które zdefiniowane zostało w treści tego dokumentu, jako:

> „Każde nielegalne działanie, które dla skutecznego ścigania wymaga wiedzy w zakresie technologii komputerowej”[199].

Dla ukonstytuowania tak określonego przestępstwa związanego z komputerem niezbędne było zatem łączne spełnienie dwóch przesłanek:

1) kwalifikowany czyn musiał być zabroniony przez dowolny przepis odrębny; oraz
2) jego skuteczne ściganie musiało wymagać wiadomości z zakresu technologii komputerowej.

Na gruncie przytoczonej definicji, przestępstwem związanym z komputerem mógł tym samym stać się każdy czyn zabroniony - niezależnie od dobra prawnie chronionego stanowiącego przedmiot jego ataku, *modus operandi* sprawcy, czy jakichkolwiek innych cech przestępstwa - o ile tylko jego ściganie wymagało określonych umiejętności od śledczych. W efekcie zastosowania wskazanej konstrukcji, zakres semantyczny definicji stał się jednak zbyt szeroki, obejmując także takie kategorie czynów niedozwolonych, które w żadnym razie nie dotyczyły nowoczesnych technologii teleinformatycznych. Przede wszystkim, dla zaktualizowania wymagania „wiedzy komputerowej” wystarczające było, aby w trakcie ścigania dowolnego czynu, śledczy posłużył się nowoczesnymi bazami danych, w których przechowywane są elektroniczne wersje kartotek. Dziś, działanie takie stanowi standardowy

[196] S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*. Opracowanie dostępne jest w postaci elektronicznej na stronie internetowej pod adresem: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.

[197] *Vide* przypis nr 14.

[198] W oryginale „*computer abuse*”.

[199] W oryginale „*Any illegal act for which knowledge of computer technology is essential for a successful prosecution*”, Computer Crime: Criminal Justice Resource Manual, SRI International, National Criminal Justice Information and Statistics Service, California, USA, 1979, s. XXVI. Tłumaczenie własne.

element pracy dochodzeniowo-śledczej. Przestępstwem związanym z komputerem mógł być także każdy czyn, dla którego źródłem materiału dowodowego były dane zapisane na komputerze - na którym np. prowadzono listę nielegalnych transakcji, wcale niekoniecznie wykonywanych za pośrednictwem sieci. Nieco ironicznie, stwierdzić można także, że tak zdefiniowanym przestępstwem komputerowym mogła się nawet kradzież sprzętu komputerowego ze sklepu. Z drugiej strony, przytoczona definicja pomijała nowe, specyficzne formy przestępstw, które powstały dopiero z chwilą rozwinięcia sieci oraz świadczonych za ich pośrednictwem usług, jak choćby wielokrotnie przytaczane ataki typu *dos, ddos, man-in-the-middle, cache poisoning*, czy *pharming* (opisane dalej, w części szczegółowej pracy). Tak sformułowany zakres semantyczny definicji stanowił zatem rozwiązanie zupełnie nieefektywne, które nie tylko obejmowało zbyt wiele czynów, ale także nie pozwalało na dokonanie wyróżnienia żadnych cech szczególnych *przestępczości związanej z komputerem*. Pomimo przedstawionych wad przyjętej konstrukcji, analogiczne rozwiązanie wprowadzone zostało także do kolejnego - choć późniejszego, bo wydanego już w 1989 r., opracowania Ministerstwa Sprawiedliwości USA[200]. Powtórna implementacja sformułowania stworzonego oryginalnie jeszcze w połowie lat siedemdziesiątych, spotkała się jednak z gruntowną krytyką[201]. Ostatecznie, należy zauważyć, że w dobie postępującej informatyzacji, coraz mniej czynności realizowanych jest z wykluczeniem jakiegokolwiek udziału systemów teleinformatycznych, co nie powinno jednocześnie oznaczać logicznego przeniesienia całej przestępczości do sfery cyberprzestrzeni. Definicja odwołująca się do *obszaru przestępczości komputerowej*, powinna przy tym umożliwiać precyzyjne wydzielenie działalności tego typu spośród innych form przestępczości. W innym przypadku, tworzenie nowych, szczególnych regulacji prawnych - tak materialnych, jak i procesowych, nastawionych na walkę z nowoczesnymi zagrożeniami, stałoby się niemożliwe.

Wyrażenie „przestępstwo związane z komputerem" wykorzystywane było w kolejnych latach także na gruncie licznych aktów międzynarodowych, które proponowały swoje definicje tego pojęcia. Przykładowo, na potrzeby wydanego przez Komitet Ministrów Rady Europy w 1989 r. Zalecenia Nr R(89)9[202] w sprawie przestępczości związanej

[200] *Computer Crime: Criminal Justice Resource Manual, U.S. Department of Justice, National Institute of Justice*, 1989.

[201] Np. M. Goodman, *Making Computer Crime Count*, FBI *Law Enforcement Biulettin*, August 2001, s. 12. Biuletyn dostępny na stronie internetowej pod adresem: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2001-pdfs/aug01leb.pdf. Także: R. W. Aldrich, Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime. Materiał dostępny na stronie internetowej pod adresem: http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf.

[202] *Council of Europe, Computer-Related Crime: Recommendation No. R (89)9 on computer-related crime and final report of the European Committee on Crime Problems*, Strasburg 1989.

z komputerami - przygotowująca dokument grupa ekspertów postanowiła określić znaczenie analizowanego pojęcia poprzez stworzenie jego typologii, a zatem budując katalog czynów, nie zaś określając ich cechy rodzajowe. Jako uzasadnienie dla odstąpienia od budowy klasycznej definicji pojęcia, wskazane zostały trudności w wypracowaniu wspólnego, jednolitego sposobu postrzegania tego typu przestępczości. W efekcie, w Zaleceniu z 1989 r. wymieniono te kategorie czynów, które powinny być penalizowane właśnie jako *przestępstwa związane z komputerem.* Do czynów obligatoryjnie kwalifikowanych w ten sposób (znajdujących się na tzw. liście minimalnej - obligatoryjnej) zaliczone zostały wówczas: oszustwo związane z komputerem, fałszerstwo komputerowe, uszkodzenie danych lub programów, sabotaż komputerowy, nieuprawniony dostęp do zasobów, nieuprawniony podsłuch, bezprawne powielanie chronionych programów komputerowych oraz bezprawne powielanie topografii półprzewodników. Dodatkowo, wskazano także cztery kolejne kategorie przestępstw, co do których nie osiągnięto pełnego konsensusu w zakresie ich kwalifikowania do katalogu *przestępstw związanych z komputerem*, tworząc tzw. listę opcjonalną. Na liście tej znalazły się w efekcie: nieuprawniona modyfikacja danych lub oprogramowania, szpiegostwo komputerowe, wykorzystywanie komputera bez zezwolenia oraz nieuprawione używanie programu komputerowego[203]. Z wyjątkiem bezprawnego kopiowania topografii półprzewodników, wszystkie wymienione kategorie działań odniesione zostały bezpośrednio do obszaru szeroko rozumianego przetwarzania danych, łącząc – w sposób charakterystyczny dla dawniejszych dokumentów, sfery *stricte* karną oraz ochrony praw autorskich. Typologia nie wprowadzała także podziału na specjalistycznie wyodrębnione ataki komputerowe, starając się uzyskać bardziej definicyjny, ogólny charakter. Warto zaznaczyć, że pomimo istotnego oparcia się przywołanego dokumentu Rady Europy na ustaleniach wcześniejszego, pochodzącego z połowy lat osiemdziesiątych raportu Organizacji Rozwoju i Współpracy Gospodarczej (OECD), zatytułowanego „Przestępstwa związane z komputerem: analiza polityki legislacyjnej”[204], wcześniejsze opracowanie międzynarodowe - co zostało już zaznaczone, posługiwało się określeniem *nadużycia komputerowego* nie zaś *przestępstwa związanego z komputerem*.

Pojęcie *przestępstwa związanego z komputerem* (*computer-related crime*) obecne było także w regulacjach ONZ, m. in. w zatytułowanej właśnie tym wyrażeniem rezolucji z 1990 r., przyjętej przez VIII Kongres ONZ w sprawie Zapobiegania Przestępczości oraz

---

[203] Council of Europe, Computer-Related Crime: Recommendation No. R (89)9, s. 36 i nast.
[204] *Computer-related crime: Analysis of legal policy*, OECD, Paryż 1986.

Postępowania z Przestępcami[205]. Rezolucja nie tylko nie oferowała jednak żadnej definicji pojęcia, ale wprowadzała także inne, nieznane dotąd, choć również niedefiniowane tu wyrażenia „nadużycia komputerów”[206] (w opozycji do „nadużycia komputerowego”) oraz „nadużycia związanego z komputerem”[207]. Jednocześnie, pojęcia ta traktowane były najwyraźniej synonimicznie. Pomimo niespójności oraz nieokreśloności przyjętej siatki pojęciowej, rezolucja wskazywana jest często, jako istotny wyraz zaangażowania ONZ w problematykę przeciwdziałania nowoczesnym formom przestępczości. Podkreślane są w szczególności jej ponad europejski zasięg, stawiający poruszany temat na arenie globalnej oraz proponowane w treści rezolucji kierunki działań - m. in. konieczność uzupełnienia prawodawstwa o nowe rodzaje czynów bezprawnych[208]. Chaotyczność zastosowanej na gruncie rezolucji siatki pojęciowej uznać należy jednak za istotną wadę opracowania, które stawiając sobie, jako jeden z głównych celów, identyfikację niedostatków obowiązującego prawa, nie określało jednoznacznie samego przedmiotu prowadzonej analizy. Wyrażenie „przestępstwo związane z komputerem” wykorzystane zostało następnie przez ONZ także w kolejnym opracowaniu tej organizacji - w wydanym w 1994 r. podręczniku. Dokument ten został poddany analizie w kolejnym punkcie rozdziału.

3. Pojęcie „bezprawnego użycia komputera”.

Pojęcie „bezprawnego użycia komputera” pochodzi z wydanej w 1990 r. brytyjskiej ustawy *Computer Misuse Act*[209], będącej pierwszą na wyspach - choć nadal obowiązującą, kodyfikacją prawa nakierowaną na zwalczanie przestępstw popełnianych z użyciem komputera. Przedmiotowa ustawa wprowadziła do zasobu angielskiego języka prawnego nowe, nieznane dotąd w doktrynie określenie „bezprawnego użycia komputera” (w oryginale *computer misuse*), które znaczeniowo zastępować miało inne, rozpoznawane już na arenie międzynarodowej wyrażenia, jak „nadużycie komputerowe”, czy „przestępczość związana z komputerem”. Z uwagi na kwestie językowe, niezbędne w tym miejscu staje się poczynienie

---

[205] Rezolucja opublikowana w: *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August - 7 September 1990: report prepared by the Secretariat, United Nations publication, Sales No. E.91.IV.2*), sekcja C, rezolucja nr 9, s. 140 i nast. Pełny tekst raportu dostępny na stronie internetowej pod adresem: http://www.asc41.com/UN_Congress/8th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/026%20ACONF.144.28.Rev.1%20Eighth%20United%20Nations%20Congress%20on%20the%20Prevention%20of%20Crime%20and%20the%20Treatment%20of%20Offenders.pdf

[206] W oryginale *„abuse of computers”*.

[207] W oryginale *„computer-related abuse”*.

[208] Na cechy te wskazuje m. in. A. Adamski w: A. Adamski, Prawo karne... op. cit., s. 9 - 10.

[209] *Computer Misuse Act 1990*. W tłumaczeniu „Ustawa o bezprawnym użyciu komputera z 1990 r.”. Tłumaczenie własne. Pełny, oryginalny tekst aktu dostępny na stronie internetowej parlamentu brytyjskiego, pod adresem: http://www.legislation.gov.uk/ukpga/1990/18/enacted.

uwagi o charakterze technicznym - anglojęzyczne wyrazy „*misuse*” oraz „*abuse*” (wykorzystywane odpowiednio w dwóch różnych wyrażeniach: „*computer misuse*” oraz „*computer abuse*”), tłumaczyć można synonimicznie jako „nadużycie”[210]. Tym samym, na gruncie językowym, polskojęzyczna kategoria „nadużycia komputerowego” mogłaby obejmować łącznie pojęcia „*computer abuse*” (opisane wcześniej), jak i poruszane tu „*computer misuse*”, choć z punktu widzenia prawnego, błędnie stawiałoby to znak równości pomiędzy zwrotami, zachowującymi w oryginale różne brzmienia. Dla uniknięcia takiej sytuacji, zwrot „*computer misuse*” przetłumaczony został w niniejszej pracy, jako „bezprawne użycie komputera”, mając na uwadze brytyjskie rozumienie prawniczego zwrotu „*misuse*” oraz przypadki jego występowania na gruncie angielskiego ustawodawstwa[211].

Z uwagi na brak ustawowej definicji analizowanego pojęcia, znaczenie „bezprawnego użycia komputera” musi być rekonstruowane w oparciu o typologię charakteryzowanych w ustawie czynów zabronionych. Podobnie jak w przypadku amerykańskiej ustawy karnej z 1986 r., także ustawa brytyjska skonstruowana została w typowo kodeksowy sposób (np. „kto uzyskuje...”), a typizowane w niej czyny nie zostały nazwane żadnymi określeniami rodzajowymi (np. *hacking*) - tak, jak Kodeks karny nie posługuje się wyrażeniami „zabójstwo”, czy „morderstwo”. W ustawie brytyjskiej znaleźć zatem można wyłącznie opisy poszczególnych typów przestępstw, zawarte w hipotezach przepisów. W oryginalnym kształcie, angielska ustawa przewidywała penalizację trzech następujących kategorii czynów:

1) nieuprawniony, umyślny dostęp do zasobów komputera, polegający na użyciu jakiejkolwiek funkcji komputera z zamiarem zabezpieczenia dostępu do jakiegokolwiek programu lub danych przechowywanych na jakimkolwiek komputerze;
2) nieuprawniony dostęp, o którym mowa w pkt 1, z zamiarem popełnienia lub ułatwienia popełnienia dalszych przestępstw dowolnej osobie, w dowolnym czasie;
3) nieuprawniona modyfikacja zasobu komputerowego, dokonywana w celu zakłócenia poprawnego funkcjonowania jakiegokolwiek komputera, uniemożliwienia lub

[210] Tak np. internetowy słownik Mirriam-Webster, dostępny na stronie internetowej pod adresem: http://www.merriam-webster.com/dictionary/misuse.

[211] Wyraz „*misuse*” wykorzystywany jest m.in. przez brytyjską ustawę antynarkotykową *Drugs Misuse Act 1986*. Ustawa ta porusza kwestie nie tylko samego używania środków odurzających, ale także ich produkcji, czy sprzedaży - wykraczając tym samym poza zakres rozumienia polskiego wyrażenia „nadużywanie narkotyków”.

utrudnienia dostępu do programu a także zakłócenia działania programu lub naruszenia wiarygodności danych[212].

Zgodnie z wyraźnym brzmieniem ustawy, każdy z wyżej wymienionych czynów może być popełniony w stosunku do dowolnego komputera, dowolnego programu lub danych, lub programu lub danych określonego rodzaju[213].

Wymienione w punktach 1 - 3 rodzaje czynów zabronionych sprowadzają się do dwóch, następujących kategorii działań bezprawnych: uzyskiwania lub zabezpieczania na przyszłość możliwości uzyskania nieuprawnionego dostępu do zasobów komputera, oraz dokonywania nieuprawnionych modyfikacji danych w przetwarzanych w postaci elektronicznej zasobach komputera. Pierwsza kategoria przestępstw obejmuje czyny takie jak klasyczny *hacking*, kradzież oraz wyłudzanie haseł (*phishing*), czy rozsyłanie form oprogramowania złośliwego, pozwalającego na przejęcie kontroli nad zainfekowanym komputerem. Druga grupa czynów - nieuprawniona modyfikacja danych, może lecz nie musi wiązać się z uprzednim bezprawnym uzyskaniem dostępu do określonego systemu. Wprowadzanie nieuprawnionych zmian w danych może być bowiem dokonywane także przez osobę uprawnioną do korzystania z danego komputera, lecz nieposiadającą uprawnień do dokonywania w systemie tego typu operacji. Jako nieuprawnioną zmianę należy także zawsze traktować każdy czyn skierowany przeciwko wiarygodności dokumentów. Dla uznania wystąpienia nieuprawnionej zmiany nie ma także znaczenia fakt, czy zmiana miała charakter permanentny, czy wyłącznie czasowy. Oryginalne brzmienie przepisów nie obejmowało swoim zakresem - niezwykle popularnych dziś, tzw. ataków odmowy dostępu (*dos* oraz *ddos* - opisane w dalszej części pracy) polegających w uproszczeniu na wielokrotnym odwoływaniu się do jednego zasobu w celu sparaliżowania ruchu sieciowego. Brak ten zostało uzupełniony w drodze nowelizacji z 2006 r. Ustawa brytyjska nie przewiduje natomiast szczególnych rozwiązań karnych dotyczących m. in. przechwytywania treści przekazywanych danych (podsłuch komputerowy), czy prowadzenia szczególnych form działalności szpiegowskiej. Wysoki stopień ogólności przytoczonych przepisów materialnych powoduje wreszcie konieczność dokonywania szerokich subsumcji, wprowadzających bardzo wielu różnych czynów pod te same przepisy. Rozwiązanie takie nie pozwala na dokonywanie na gruncie ustawy formalnego rozróżniania ataków charakteryzujących się zupełnie różnym *modus operandi* sprawcy.

---

212 *Computer Misuse Act 1990*, art. 1 - 3.

213 W oryginale: „any particular computer; any particular program or data; or a program or data of any particular kind.”. Tłumaczenie własne. *Computer Misuse Act 1990*, art. 1 - 3.

4. Pojęcie „przestępstwa komputerowego".

Już od drugiej połowy lat siedemdziesiątych, obok wyrażenia „nadużycie komputerowe", w piśmiennictwie popularyzowane było także inne określenie dla nowego zjawiska przestępnego, przybierające formę „przestępczości komputerowej". Pojęciem tym, między innymi, posłużyli się prof. Ulrich Sieber - uważany za jednego z ojców *prawa informatycznego*, jak i August Bequai, wprowadzając je do tytułów swoich opracowań, wydanych odpowiednio w 1977[214] oraz 1978[215] roku. Prezentowane na ich gruncie ogólne rozumienie pojęcia, nie odbiegało jednak od sposobu charakteryzowania wcześniej zdefiniowanego wyrażenia „nadużycie komputerowe". W latach następnych, wyrażenie „przestępstwo komputerowe" pojawiało się także wielokrotnie w opracowaniach amerykańskich (także amerykańskiej prasie), jednak bez definicji pojęcia, która stałaby się szeroko rozpoznawana w literaturze przedmiotu.

W cztery lata po uchwaleniu przez VIII Kongres ONZ opisanej wyżej (cz. I punkt 2) rezolucji w sprawie przestępstw związanych z komputerem, Organizacja Narodów Zjednoczonych podjęła kolejną inicjatywę odnoszącą się do problematyki zwalczania nowoczesnych form przestępczości. Wyrazem tego stało się wydanie w 1994 roku „Podręcznika w sprawie zapobiegania oraz kontroli przestępstw związanych z komputerem"[216]. Dostrzegając dotychczasowe - zaznaczane już globalnie trudności występujące w ustaleniu spójnej siatki pojęciowej, a także chcąc nadać podręcznikowi możliwie uniwersalnego charakteru, ponownie odstąpiono od budowy definicji centralnego wyrażenia na rzecz zastosowania ujęcia funkcjonalnego (zastosowano zatem rozwiązanie analogiczne, jak w przypadku opracowania wydanego w 1989 r. przez Komitet Ministrów Rady Europy). Zamiast klasycznej definicji, zaproponowano zatem katalog zdarzeń, które określane miały być, co wymaga podkreślenia - zamiennie, mianem „przestępstwa związanego z komputerem" lub „przestępstwa komputerowego"[217]. Na gruncie opisywanego podręcznika ONZ oba wyrażenia stały się zatem *de facto* synonimami, nie tylko stawiając pod znakiem zapytania jakąkolwiek zasadność ich różnicowania, ale także czyniąc to wbrew przyjętym zasadom tworzenia oraz interpretacji przepisów - które jednoznacznie nakazują, aby dwóm, różnym pojęciom nadawać zawsze dwa, różne znaczenia (w opozycji do zasady

[214] U. Sieber: *Computercriminalitat und Strafrecht*, Heymann, 1977.
[215] A. Bequai: *Computer Crime*, Lexington Books, USA, 1978
[216] *United Nations Manual on the prevention and control of computer-related crime*. Tekst dostępny na stronie internetowej pod adresem: http://www.uncjin.org/Documents/EighthCongress.html.
[217] W oryginale odpowiednio: *„computer-related crime*" oraz *„computer crime*".

jedno wyrażenie - zawsze jedno i to samo znaczenie). Pomimo deklarowanej równości pojęć, dokument wyraźnie częściej posługiwał się jednak określeniem *przestępstwa komputerowego*, które użyte zostało także w kontekście podjętej próby definicji zjawiska. Dla przybliżenia zakresu semantycznego tak określonej kategorii czynów, w punkcie 22. opracowania wprowadzona została *quasi*-definicja stanowiąca, że

> „Przestępstwo komputerowe może polegać na podejmowaniu tradycyjnych w swojej naturze działań przestępnych, takich jak kradzież, oszustwo, fałszerstwo oraz wyrządzanie szkód, które zasadniczo wszędzie podlegają sankcji karnej. Komputery wytworzyły jednak także szereg nowych, potencjalnych działań bezprawnych lub możliwości nadużyć, które mogą, lub powinny być uważane za przestępstwa."[218].

Przytoczona definicja w sposób czytelny zwraca uwagę na rozróżnienie dwóch głównych kategorii czynów, które mogą podpadać pod miano „przestępczości komputerowej". Z jednej strony są to „tradycyjne z natury" działania przestępne, dla których komputer staje się nowym narzędziem przestępstwa (w tym tworzy nowe, specyficzne środowisko do ich popełniania), z drugiej zaś - zupełnie nowe typy czynów bezprawnych, niepoddające się subsumcji pod obowiązujące przepisy karne. W uzupełnieniu, podręcznik podkreślał też, że komputer może stać się nie tylko narzędziem, ale także przedmiotem - czy innymi słowy celem, tak określonego czynu. Zaprezentowane rozróżnienie na kategorie typowych oraz nowych form przestępstw, stało się w kolejnych latach cechą charakterystyczną pojęcia „przestępstwa komputerowego".

Poza przytoczoną definicją podręcznik prezentował także katalog typowych przestępstw komputerowych, w którym zawarte zostały następujące kategorie czynów: oszustwo przez komputerową manipulację (odnoszące się do zaburzenia poprawnego funkcjonowania urządzenia), fałszerstwo komputerowe, uszkodzenie lub modyfikacja przetwarzanych danych lub oprogramowania, nieuprawniony dostęp do systemu komputerowego lub usługi oraz nieuprawnione powielanie chronionego prawem programu komputerowego. Pomimo przyjęcia nieco innego nazewnictwa, przedstawiony katalog pozostawał w istocie zbieżny z listą przestępstw stworzoną osiem lat wcześniej przez ekspertów OECD na potrzeby wydanej przez tę organizację analizy polityki legislacyjnej. Zważywszy na niezwykłe tempo rozwoju technologicznego oraz podążający za nim krok, w krok, rozwój form i metod nowoczesnej przestępczości, brak nowych, precyzyjnych

---

[218] W oryginale: *Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions. The computer has also created a host of potentially new misuses or abuses that may, or should, be criminal as well*. Tłumaczenie własne.

przepisów spełniających standardy prawa karnego, uznać należy za przejaw nienadążania regulacji za wymaganiami, jakie stawia otaczająca nas rzeczywistość. Korzystanie z już przyjętych rozwiązań, podkreśla równocześnie, jak trudnym zadaniem jest wypracowywanie na arenie międzynarodowej kompromisów w odniesieniu do tworzenia nowych, wspólnych regulacji karnych.

Przenosząc się na grunt krajowy, pojęciem „przestępstwa komputerowego" posłużył się także prof. A. Adamski, zawierając je w swoim opracowaniu zatytułowanym „Prawo karne komputerowe"[219]. Pozycja ta, choć wydana w 2000 r., uznawana jest za kanon polskich rozważań prawniczych w przedmiocie charakteryzowania zjawiska przestępczości komputerowej, w ostatnich latach poszerzanych oraz odświeżanych na gruncie zmieniającego się otoczenia prawnego[220]. Zwracając uwagę na istotne wady siatki terminologicznej stosowanej w obszarze prawa karnego komputerowego, prof. A. Adamski zaprezentował własną, poszerzoną charakterystykę pojęcia „przestępstwa komputerowego", wprowadzając podział definicyjny przestępczości komputerowej na dwa odrębne ujęcia: materialno-prawne oraz procesowe. W ramach ujęcia materialno-prawnego - stosując kryterium roli, w jakiej występować mogą komputery w działaniu przestępnym, wyróżnione zostały w dalszej kolejności dwie subkategorie przestępczości komputerowej - w rozumieniu wąskim (tzw. przestępstwa *stricte* komputerowe) oraz w rozumieniu szerokim:

– przestępstwami *stricte* komputerowymi prof. A. Adamski nazwał te czyny bezprawne, które skierowane są przeciwko systemom, danym, lub programom - czyli czyny, w których nowoczesne technologie informatyczne stanowią bądź to sam przedmiot zamachu, bądź też środowisko do jego przeprowadzenia. Jak zauważa autor, następuje w tym przypadku swoiste genetyczne powiązanie nowoczesnych form przestępczości z technologią komputerową. Przestępstwa należące do tej kategorii należy odnosić do czynów naruszających tzw. atrybuty bezpieczeństwa danych - w szczególności ich poufność, integralność oraz dostępność. Cechy te oznaczają odpowiednio, że przetwarzane w systemach teleinformatycznych dane nie zostały ujawione osobom nieuprawnionym (zdarzenie nazywane także kompromitacją danych); nie zostały w sposób nieuprawniony zmodyfikowane lub uszkodzone; oraz, są dostępne dla uprawnionych użytkowników, zgodnie z zasadami panującymi w danym systemie

[219] A. Adamski, Prawo karne... op. cit., s 30 i nast.
[220] Np. praca zbiorowa pod red. W. Filipkowskiego, E. W. Pływaczewskiego oraz Z Rau, Przestępczość w XXI wieku - zapobieganie i zwalczanie. Problemy technologiczno-informatyczne, Wolters Kluwer, Wyd. I, 2015, czy też J. Kosiński (pod red.), Przestępczość teleinformatyczna 2015, Szczytno 2015.

(np. nie dokonano przeciążenia łączy, co uniemożliwiałoby odwołanie się do danego zasobu),

- przestępstwami komputerowymi w ujęciu szerokim nazwane zostały zaś te wszystkie czyny, których ustawowa regulacja wprowadza *expressis verbis* użycie komputera do ich popełnienia, np. przestępstwa z art. 130 § 3, 267 - 269, 278 § 2, 285, czy 287 obowiązującego Kodeksu karnego. Jak zauważa prof. A. Adamski, są to przestępstwa komputerowe „nie ze względu na przedmiot zamachu, lecz ustawowo określony sposób działania sprawcy”[221]. Dobrem prawnie chronionym nie jest tutaj samo funkcjonowanie systemu, lecz różne inne dobra. Przestępstwa należące do tej grupy, prof. A. Adamski sugeruje nazywać *przestępstwami komputerowymi* z dodaniem określenia przedmiotu ochrony, np. „przestępstwo komputerowe przeciwko wiarygodności dokumentów”.

Istotnym uzupełnieniem zaprezentowanego podziału, jest także sposób uwzględnienia pozostałych czynów (nienależących do żadnej z kategorii przestępstw komputerowych), w których komputer może jednak wystąpić faktycznie w roli narzędzia do popełnienia „klasycznego” przestępstwa, np. przestępstwa zniewagi, zniesławienia, groźby karalnej, propagacji treści prawnie zabronionych, czy oszustwa. Dla tej kategorii zdarzeń, prof. A. Adamski przyjmuje nazwę „przestępstwa popełniane z użyciem (wykorzystaniem) komputera”. Mianem tym określane są zatem te czyny, których ustawowa regulacja nie zakłada użycia komputera, jako przesłanki konstytuującej czyn, lecz możliwe jest ich popełnienie także właśnie z zastosowaniem systemów teleinformatycznych (szczególny, lecz niewymagany przepisem rodzaj *modus operandi* sprawcy).

W ujęciu procesowym, przestępstwami komputerowymi określono zaś na gruncie opracowania:

> „[...] wszelkie czyny zabronione przez prawo karne, których ściganie wymaga od organów wymiaru sprawiedliwości uzyskania dostępu do informacji przetwarzanej w systemach komputerowych lub teleinformatycznych. Pojęcie przestępstw komputerowych w aspekcie procesowym obejmuje zatem zarówno przypadki, w których system komputerowy stanowi przedmiot, jak i narzędzie zamachu.”[222].

W ujęciu procesowym, przestępstwem komputerowym będzie zatem każdy czyn, w którym komputer może dostarczyć dowodów niezbędnych do jego ścigania.

---

[221] *Ibidem*, s. 31 i 32.
[222] *Ibidem*, s. 34.

Topografię przyjętego podziału można zatem zobrazować następującym schematem:

I. Przestępstwa w ujęciu materialno-karnym:
   1) przestępstwa *stricte* komputerowe (system, jako cel lub środowisko);
   2) przestępstwa, w których użycie komputera stanowi element opisu czynu (przesłanka obligatoryjna) - tzw. przestępstwa komputerowe przeciwko określonemu dobru prawnie chronionemu; oraz,
   3) przestępstwa „klasyczne", które mogą zostać popełnione przy wykorzystaniu komputera - tzw. przestępstwa z użyciem komputera.

II. Przestępstwa w ujęciu procesowym:
   – przestępstwa, w których komputery stanowią podstawowe źródło materiału dowodowego.

Zaprezentowana przez prof. A. Adamskiego charakterystyka zjawiska przestępczości komputerowej nie tylko zaznacza różne role, w jakich może występować komputer, ale zwraca również uwagę na zasadność wielopoziomowego definiowania opisywanego zjawiska. W czasach pełnego rozkwitu technologii informatycznych, gdy kolejne *tradycyjne* przestępstwa odnajdują swoją drogę do cyberprzestrzeni, jedynie bowiem taki sposób analizy pozwala na stworzenie pełnego obrazu tego, czym jest przestępczość komputerowa, składająca się *de facto* z klasycznych, jak i zupełnie nowych form działalności przestępnej. Kwestie te winny być ponadto ujmowane tak od strony materialno-prawnej, jak również procesowej, co znajduje wyraz w dwóch opisanych ujęciach.

Choć w tym miejscu jedynie sygnalizacyjnie, warto nadmienić, że w swoich późniejszych opracowaniach tematu - zawierających się w artykułach drukowanych w piśmiennictwie prawniczym, prof. A. Adamski wykorzystuje także analizowane w dalszej części rozdziału pojęcie „cyberprzestępczości"[223].

5. Pojęcie „przestępstwa powiązanego z technologią informacyjną".

Pojęcie „przestępstwa powiązanego z technologią informacyjną" - przyjmujące w oryginale brzmienie *„Offence connected with Information Technology"*[224], zdefiniowane zostało w związku z pracami prowadzonymi nad Zaleceniem Nr (95) 13 Komitetu Ministrów Rady Europy z 1995 r. w sprawie „Problemów prawa karnego procesowego związanych

---

[223] Tak np. w A. Adamski, Cyberprzestępczość - aspekty prawne i kryminologiczne, Studia Prawnicze Nr 4 z 2005 r., s. 51 i nast.

[224] W skrócie też *„IT offence"* - „przestępstwo dotyczące IT".

z technologią informacyjną"[225]. Dokument ten stał się pierwszym istotnym wyrazem międzynarodowego zainteresowania problematyką podejmowania czynności procesowych - ze szczególnym uwzględnieniem ich roli dowodowej, w kontekście zwalczania nowoczesnych form przestępczości[226]. Analiza zawartej w dokumencie definicji pozwoli zatem zaprezentować ujęcie, które zostało stworzone specyficznie z myślą o zagadnieniach karnoprocesowych. Zgodnie z memorandum wyjaśniającym (*explanatory memorandum*), stanowiącym funkcjonalne uzupełnienie treści samego Zalecenia, „przestępstwem powiązanym z technologią informacyjną" jest:

> „Każde przestępstwo, w którego procesie śledczym właściwe organy wymiaru sprawiedliwości muszą uzyskać dostęp do informacji przetwarzanych lub przekazywanych w systemach komputerowych lub [...] systemach przetwarzania danych występujących w postaci elektronicznej."[227]

Na potrzeby opracowania, pojęcia „systemów komputerowych" oraz „systemów przetwarzania danych" rozumiane były możliwie szeroko, obejmując w zasadzie wszelkie przykłady technologii informacyjnych, w tym zarówno pojedyncze (odseparowane od środowiska cyfrowego) komputery, jak i całe sieci. Jak można przeczytać we wprowadzeniu do definicji, systemy w tak zdefiniowanym przestępstwie, mogą występować w następujących rolach:

1) system, jako narzędzie do popełnienia przestępstwa;
2) system, jako przedmiot (cel) przestępstwa;
3) system, jako środowisko dla popełnienia przestępstwa; oraz,
4) system, jako środowisko, w którym pojawić się mogą dowody przestępstwa - w tym przypadku, sam system nie musi stanowić żadnego elementu w procesie popełniania przestępstwa.

Analizując przytoczoną wyżej definicję „przestępstwa powiązanego z technologią informacyjną", podkreślić trzeba jej silne zorientowanie na kwestię dowodową. Przestępstwo nie jest tu definiowane przez pryzmat materialno-prawny, czy ujęcie *modus-operandi* jego sprawcy, lecz z punktu widzenia potencjalnego źródła dowodowego, mogącego dostarczyć informacji o przestępstwie. *Przestępstwem powiązanym z technologią informacyjną* - co na

---

[225] Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology and Explanatory Memorandum, Council of Europe Publishing, 1996.

[226] A. Adamski, Prawo karne... op. cit., s. XVII.

[227] W oryginale: „*Any criminal offence , in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer systems, or, as they are referred to above, electronic data processing systems.*". Tłumaczenie własne.

gruncie definicji wyrażone zostało wprost, może bowiem stać się potencjalnie każdy czyn bezprawny, o ile tylko szeroko rozumiane systemy teleinformatyczne mogą dostarczyć dowodów jego wystąpienia. Definicję uzupełniają zatem w istotny sposób zawarte w dokumencie rozważania odnoszące się do ról, w których występować mogą same systemy. Analogicznie bowiem do nich, wykrywane dowody przybierać będą określoną treść oraz formę. Dla przykładu, w przypadku systemu-narzędzia, dowód przestępstwa wskazywać będzie musiał szczegółowo na sposób bezprawnego wykorzystania systemu oraz nadużycia jego technicznych możliwości; w przypadku systemu-środowiska, dowodem będzie z kolei np. zapis znieważającego wpisu, który zamieszczony został na publicznie dostępnej stronie internetowej. Niezależnie od wskazanej korelacji pomiędzy rolą systemu a treścią (a co za tym idzie, także rolą) elektronicznego dowodu popełnienia *przestępstwa związanego z technologią informacyjną*, pozyskiwane dowody - o których traktuje definicja, w każdym przypadku przybierać będą postać cyfrowych danych przetwarzanych w szeroko rozumianych systemach teleinformatycznych.

6. Pojęcie „cyberprzestępstwa”.

Wyrażenie „cyberprzestępstwo”, przyjmujące w angielskim oryginale brzmienie *„cybercrime”*, stanowi aktualnie jedno z najszerzej rozpoznawanych pojęć używanych dla określenia nowoczesnych form przestępczości komputerowej. Swoją rangę zawdzięcza w największej mierze Konwencji Rady Europy o cyberprzestępczości[228], zwanej też czasami Konwencją z Budapesztu[229], stanowiącej wynik jednej z najistotniejszych inicjatyw międzynarodowych odnoszących się do regulacji kwestii zwalczania przestępczości komputerowej. Konwencja została otwarta do podpisu 23 listopada 2001 r., zaś weszła w życie 1 lipca 2004 r. po uzyskaniu ratyfikacji pięciu państw (wymogiem było ażeby przynajmniej trzy z nich należały do Rady Europy). Łącznie Konwencja została podpisana przez 47 państw, w tym Polskę, która stała się sygnatariuszem dokumentu już w dniu jego otwarcia do podpisu[230]. Pośród istotnych sygnatariuszy Konwencji wskazać należy między innymi Anglię, Niemcy, Francję, Szwecję, Rosję a także Stany Zjednoczone, czy Japonię[231].

[228] Tytuł oryginalny: *Convention on Cybercrime*, CETS Nr: 185. Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[229] Tak np. na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Convention_on_Cybercrime.

[230] Aktualne informacje dotyczące sygnatariuszy można znaleźć na oficjalnej stronie internetowej Konwencji, dostępnej pod adresem: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp? NT=185& CM=1&DF=&CL=ENG.

[231] Konwencję podpisały w sumie cztery państwa nie będące członkami Rady Europy, choć z grupy tej ratyfikowało ją wyłącznie USA (w dniu 29 września 2006 r., Konwencja weszła zaś w życie w USA z dniem 1 stycznia 2007 r.).

W dniu 28 stycznia 2003 r. w Strasburgu otwarty do podpisu został także Protokół Dodatkowy do Konwencji dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych[232]. Protokół wszedł w życie 1 marca 2006 r. (po uzyskaniu pięciu ratyfikacji). Polska podpisała protokół w dniu 21 lipca 2003 r.[233].

Choć Polska nie dokonała oficjalnej ratyfikacji Konwencji oraz protokołu dodatkowego aż do roku 2015 (oficjalnie konwencja weszła w życie z dniem 1 czerwca 2016 r.)[234], krajowe ustawodawstwo karne zostało dostosowane do jej postanowień znacznie wcześniej, w szczególności na mocy ustawy z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń[235]. Rozwiązania prawnokarne przyjęte na gruncie krajowym poddane zostały analizie, zgodnie z przyjętym tokiem wywodu, w rozdziale IV.

Przechodząc do szczegółowego przybliżenia przepisów Konwencji z Budapesztu, w pierwszej kolejności należy zauważyć, że dokument ten nie wprowadza definicji pojęcia „cyberprzestępstwo", nakazując tym samym rekonstrukcje jego znaczenia na podstawie opisanych w akcie rodzajów czynów zabronionych. Podobnie, jak w przypadku wielu innych dokumentów także i tu zastosowane zostało tzw. ujęcie funkcjonalne, skupiające się na opisach hipotez czynów, które winny być penalizowane w systemach prawnych państw - stron umowy oraz tworzeniu katalogów takich czynów. Samo wyrażenie „cyberprzestępstwo" (lub też „cyberprzestępczość" - oryginalny zwrot *„cybercrime*" może być bowiem stosowany w obydwu kontekstach) pada w Konwencji dziewięciokrotnie, przy czym tylko raz w samej treści postanowień aktu (w kontekście współpracy międzynarodowej), zaś pozostałe osiem razy w preambule, nie stanowiącej materiału normatywnego. Z zastosowaniem kryterium dobra prawnie chronionego będącego przedmiotem ataku, czyny stypizowane w Konwencji podzielone zostały na cztery kategorie (wskazane w tytułach 1 - 4 rozdziału II Konwencji): przestępstwa przeciwko poufności, integralności oraz dostępności danych oraz systemów

[232] Tytuł oryginalny: *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, CETS Nr: 189. Pełny tekst protokołu dostępny jest na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

[233] Aktualne informacje dotyczące sygnatariuszy protokołu można znaleźć na oficjalnej stronie internetowej Konwencji, dostępnej pod adresem: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG.

[234] Ustawa ratyfikacyjna z dnia 12 września 2014 r., Dz. U. poz. 1514. Tekst Konwencji został podany do powszechnej wiadomości Przez Prezydenta RP w dniu 27 maja 2015 r., Dz. U. z 2015 r. poz. 728. Konwencja weszła w życie z dniem 1 czerwca 2016 r. Tekst protokołu dodatkowego został podany do powszechnej wiadomości ustawą z dnia 27 maja 2015 r., Dz. U. z 2015 poz. 730.

[235] Dz. U. z 2004, Nr 69, poz. 626.

komputerowych[236] (w przekładzie zawartym w ustawie ratyfikacyjnej „przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów"); przestępstwa związane z komputerami[237] (w oficjalnym przekładzie „przestępstwa komputerowe"); przestępstwa związane z przetwarzanymi treściami[238] („przestępstwa ze względu na charakter informacji"); oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych[239]. Co wymaga podkreślenia - w ocenie Autora niniejszej pracy, przyjęte w oficjalnym przekładzie tekstu Konwencji wyrażenia w sposób istotny odbiegają od ich tłumaczenia językowego, czego powodem może być w szczególności próba odniesienia tekstu Konwencji opublikowanego w Dzienniku Ustaw do siatki pojęciowej ustaw krajowych. Z uwagi jednak na definicyjny charakter niniejszego rozdziału, a także komparatystyczny cel przywoływania postanowień Konwencji, w prowadzonej tu analizie stosowane będą wyrażenia Konwencji zarówno pochodzące z przekładu oficjalnego, jak również - pierwszorzędnie, wynikające z tłumaczenia własnego, które zostało wykonane przy możliwie dużym zachowaniu oryginalnego charakteru pojęć Konwencji.

Klasyfikację poszczególnych czynów składających się na pojęcie „cyberprzestępstwa" prezentuje poniższy schemat:

I. Przestępstwa przeciwko poufności, integralności oraz dostępności danych oraz systemów komputerowych (w oficjalnym tłumaczeniu „przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów"):
   1) Nielegalny dostęp - rozumiany, jako dostęp do całości lub części systemu bez posiadania uprawnień dla takiego działania;
   2) Nielegalne przechwytywanie danych - rozumiane, jako przechwytywanie wszelkich transmisji danych komputerowych, nieposiadających charakteru publicznego, w tym przechwytywanie ulotu elektromagnetycznego (czym jest ulot wyjaśniono w rozdziale III pracy);
   3) Zakłócanie danych (w wersji polskiej Konwencji „naruszenie integralności danych") - rozumiane, jako formy niszczenia danych poprzez uszkadzanie (w przekładzie „niszczenie"), kasowanie, pogarszanie (w oryginale

[236] W oryginale: „ *Offences against the confidentiality, integrity and availability of computer data and systems*". Tłumaczenie własne.
[237] W oryginale: „*Computer-related offences*". Tłumaczenie własne.
[238] W oryginale: „*Content-related offences*". Tłumaczenie własne.
[239] W oryginale: „*Offences related to infringements of copyright and related rights*".

„*deteriorating*"), zmienianie lub utrudnianie dostępu do danych komputerowych (w oficjalnym przekładzie - „ukrywanie")[240];

4) Zakłócanie systemów (w wersji polskiej Konwencji „naruszenie integralności systemu") - rozumiane, jako istotne zakłócenie funkcjonowania systemu komputerowego dokonywane poprzez wprowadzanie, transmisję, uszkadzanie, kasowanie, pogarszanie, zmienianie lub czyszczenie danych komputerowych;
5) Niewłaściwe użycie urządzenia, w tym także oprogramowania lub kodu dostępu - rozumiane, jako posiadanie, wytwarzanie, handel lub inne formy udostępniania urządzeń lub programów zaprojektowanych lub przystosowanych do popełniania czynów wymienionych wyżej, lub też kodów dostępowych lub innych danych pozwalających na uzyskanie dostępu do całości lub części systemu komputerowego.

II. Przestępstwa związane z komputerami (w przekładzie Konwencji „przestępstwa komputerowe"):

1) Fałszerstwo związane z komputerami („fałszerstwo komputerowe") - rozumiane, jako bezprawne wprowadzenie, zmienienie, usunięcie lub utrudnianie dostępu do danych komputerowych, skutkujące ich nieautentycznością, z zamiarem wykorzystania tak przekształconych danych, jako autentyczne;
2) Oszustwo związane z komputerami („oszustwo komputerowe") - rozumiane, jako powodowanie strat majątkowych z zamiarem bezprawnego uzyskania dla siebie lub osoby trzeciej korzyści majątkowych, poprzez wprowadzenie, zmianę, usunięcie lub utrudnianie dostępu do danych komputerowych lub też zakłócenie funkcjonowania systemu komputerowego.

III. Przestępstwa związane z przetwarzanymi treściami:

– Przestępstwa związane z pornografią dziecięcą, polegające na wytwarzaniu, udostępnianiu lub posiadaniu materiałów pornograficznych z udziałem małoletniego (domyślnie Konwencja ustala granicę 18 lat, zezwalając jednak państwom na obniżenie cezury wieku do lat 16).

[240] W oryginale: „*Suppression of computer data*". Wyrażenie to odnosić należy do wszelkich działań mających na celu ograniczenie dostępu do określonych danych, jednak nie naruszających samych danych będących głównym celem ataku, np. prosta zmiana tytułu pliku powodującą niemożliwość jego automatycznego otwarcia.

IV. Przestępstwa związane z naruszeniami praw autorskich i praw pokrewnych - rozumiane, jako działania kierowane przeciwko prawom autorskim lub prawom pokrewnym, na skalę komercyjną, przy zastosowaniu systemu komputerowego[241].

Zgodnie z przyjętymi na gruncie Konwencji definicjami:

- „system komputerowy" (w przekładzie z ustawy ratyfikacyjnej „system informatyczny", w oryginale *„computer system*") to każde urządzenie lub grupa połączonych lub powiązanych urządzeń, z których przynajmniej jedno przetwarza dane w zautomatyzowany, zaprogramowany sposób,
- „dane komputerowe" (w przekładzie z ustawy ratyfikacyjnej „dane informatyczne", w oryginale *„computer data*") to wszelka reprezentacja faktów, informacji lub pojęć w formie odpowiedniej do przetwarzania w systemie komputerowym[242], w tym także oprogramowanie zdolne wykonywać określone funkcje.

Przytoczony katalog czynów zabronionych uzupełniają postanowienia przywołanego wyżej protokołu dodatkowego do Konwencji dotyczącego penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych. Dokumentem tym wprowadzono szczególną penalizację czynów dokonywanych za pośrednictwem systemów komputerowych, polegających na:

1) publicznym udostępnianiu rasistowskich oraz ksenofobicznych materiałów poprzez systemy komputerowe;
2) kierowaniu gróźb karalnych o podłożu rasowym lub ksenofobicznym, przekazywanych poprzez systemy komputerowe;
3) publicznym znieważaniu osób, dokonywanym poprzez systemy komputerowe, na tle rasistowskim lub ksenofobicznym;
4) publicznym udostępnianiu poprzez systemy komputerowe materiałów odmawiających ludziom praw lub im umniejszających na tle rasistowskim lub ksenofobicznym, a także pochwalających lub usprawiedliwiających zbrodnie ludobójstwa lub inne zbrodnie przeciwko ludzkości, zdefiniowane na mocy odpowiednich przepisów międzynarodowych;

[241] Przygotowano na podstawie art. 2 - 10 Konwencji o cyberprzestępczości. Częściowo wykorzystano tłumaczenie własne.

[242] Co warto podkreślić, oficjalne tłumaczenie Konwencji, zaraz po wprowadzeniu pojęcia „systemu informatycznego" definiuje „dane informatyczne", jako dane występujące w formie właściwej do przetwarzania w „systemie komputerowym" (nie zaś w „systemie informatycznym") - a więc w systemie, który nie został zdefiniowany.

5) udzielaniu pomocy w popełnieniu lub ułatwianiu popełnienia, któregokolwiek z powyższych czynów zabronionych[243].

Komentując powyższy katalog czynów bezprawnych, określanych łącznie - zgodnie z tytułem Konwencji, mianem „cyberprzestępstw", należy podkreślić szerokość jego zakresu przedmiotowego oraz złożoność. W pierwszej kolejności, katalog obejmuje szereg zróżnicowanych czynów, które kierowane są przeciwko różnym dobrom prawnie chronionym. Z uwagi na szerokość opisów poszczególnych czynów, ich szczegółowy *modus operandi* może ponadto przybierać rozliczne formy i treści. Po drugie zaś, przedstawiony katalog zawiera w sobie zarówno te czyny, których popełnienie możliwe jest wyłącznie w środowisku cyberprzestrzeni, jak i te, w których systemy teleinformatyczne stanowią wyłącznie narzędzie - to jest czyny, których popełnienie nie narusza samej pracy systemów, czy bezpieczeństwa przetwarzanych w nich danych. Przestępstwa propagowania pornografii dziecięcej, nielegalnego kopiowania materiałów chronionych prawem autorskim, czy udostępniania materiałów rasistowskich, także stają się cyberprzestępstwami, o ile popełnione są z zastosowaniem komputera.

Pochodzący z Konwencji oraz protokołu katalog obejmuje w efekcie wszystkie trzy grupy przestępstw komputerowych wskazane przez prof. A. Adamskiego (przestępstwa *stricte* komputerowe; przestępstwa, w których użycie komputera stanowi niezbędny element hipotezy przepisu penalizującego dany czyn; oraz przestępstwa z użyciem komputera - czyli przestępstwa, w których komputer stanowi opcjonalne narzędzie - szerzej na ten temat wyżej, w pkt 4 niniejszej części rozdziału). Na gruncie przywoływanej Konwencji, wskazane grupy czynów zaliczone zostały do wspólnej, choć nie jednolitej kategorii „cyberprzestępczości", będącej pojęciem nadrzędnym oraz zbiorczym.

Co wymaga odrębnego odnotowania, jedna z subkategorii cyberprzestępczości definiowanej na gruncie Konwencji, określona została mianem „przestępstw związanych z komputerami" (*vide* kategoria II na powyższym schemacie, w tłumaczeniu oficjalnym Konwencji określona zupełnie nietrafnie mianem „przestępstw komputerowych"), przyjmującym w oryginale brzmienie „*computer-related offences*". W bezpośrednim tłumaczeniu na język polski, pojęcie to winno przyjmować brzmienie identyczne do

[243] Przygotowano na podstawie art. 3 - 7 Protokołu Dodatkowego do Konwencji o cyberprzestępczości dotyczącego penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych. Częściowo oparto na tłumaczeniu własnym. Na marginesie warto zauważyć, iż o ile sam przekład oficjalny Konwencji wprowadza (choć jak było zauważone wcześniej - robi to niekonsekwentnie) pojęcie „systemu informatycznego", o tyle oficjalne tłumaczenie protokołu dodatkowego posługuje się zwrotem „system komputerowy", zbieżnym z oryginałem angielskim „*computer system*".

tłumaczenia wyrażenia „*computer-related crime*" - znanego z innych dokumentów źródłowych (opisane w pkt 2 niniejszego paragrafu). Jako uwagę o charakterze terminologicznym, należy zatem zaznaczyć, że na gruncie Konwencji, „przestępstwa związane z komputerami" („*computer related-offences*") stały się jedną z grup cyberprzestępczości, nie zaś samodzielną kategorią odnosząca się do wszystkich form przestępczości nowoczesnych technologii. Jako przykłady przestępstw związanych z komputerami Konwencja wskazała dwa czyny - fałszerstwo komputerowe oraz oszustwo komputerowe, które choć wywodzą się z „klasycznych" przestępstw, znanych od stuleci, aktualnie nabrały zupełnie nowego znaczenia po przetransponowaniu do cyfrowego środowiska cyberprzestrzeni, stając się *de facto* nowymi, odrębnie typizowanymi czynami.

Uzupełniająco, postanowienia Konwencji zawarte w jej preambule skupiają się na istotnych wymogach odnoszących się do skutecznego zwalczania cyberprzestępstw, zwracając uwagę między innymi na następujące zagadnienia:

- ochrona rozwiniętych społeczności przed cyberprzestępcami musi stanowić dziś jeden z priorytetów państw,
- zwalczanie cyberprzestępczości wymaga ścisłej współpracy międzynarodowej w sprawach karnych,
- niezbędne jest podjęcie współpracy pomiędzy podmiotami należącymi do administracji państwowej, a przedstawicielami szeroko rozumianej branży komputerowej.

Ostatecznie, jako ciekawostkę warto także zauważyć, że w Raporcie Wyjaśniającym[244] do Konwencji o cyberprzestępczości, sformułowanie „*cybercrime*" pojawia się jedynie raz, w odniesieniu do tytułu samej Konwencji. Raport wprowadza natomiast inne, nieznane na gruncie Konwencji Budapesztańskiej, pojęcie „czynów bezprawnych cyberprzestrzeni" lub też „przestępstwa cyberprzestrzeni"[245], odwołujące się zarówno do czynów skierowanych przeciwko integralności dostępności oraz poufności systemów komputerowych oraz sieci telekomunikacyjnych, jak i czynów zawierających w sobie element wykorzystania takich sieci oraz oferowanych przez nie usług, do popełnienia tradycyjnych przestępstw[246].

[244] *Explanatory Report*. Pełny tekst dokumentu dostępny na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.
[245] W oryginale „*cyber-space offences*". Tłumaczenie własne.
[246] *Explanatory Report*. Część II, pkt 8.

Przechodząc na grunt dokumentów krajowych, pojęcie „cyberprzestępstwa” wykorzystane zostało w następnych latach we wszystkich, pojawiających się od 2003 r., rządowych programach ochrony cyberprzestrzeni. Pojęcie „cyberprzestępstwa” wprowadzone zostało w pierwszej kolejności do programu USA (2003 r.), następnie programów Polski (2009 r.), Anglii (2009 r. oraz 2011 r.), Niemiec (2011 r.), Francji (2011 r.), a także Holandii (2011 r.). Wyrażenie „cyberprzestępstwo” pojawia się także na gruncie Polskiej „Polityki Ochrony Cyberprzestrzeni RP”, nazywanej na wcześniejszych etapach prac legislacyjnych „Rządowym Programem Ochrony Cyberprzestrzeni na lata 2011 - 2016”. Dokument ten stanowi kontynuację wcześniejszego „Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009 - 2011”. Pomimo szerokiego spektrum występowania pojęcia „cyberprzestępstwo”, jedynie dwa ze wskazanych wyżej dokumentów rządowych wprowadzają jego definicję - są nimi strategia Francuska oraz projektowana w RP Polityka.

Pochodzący z 2011 r. rządowy program Francji, zatytułowany „Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji”[247], definiuje pojęcie „cyberprzestępstwa”, jako:

> „Czyny naruszające postanowienia umów międzynarodowych lub regulacji krajowych, wykorzystujące sieci lub systemy informacyjne jako narzędzia do popełnienia deliktu lub przestępstwa, lub jako cel bezprawnego zamachu.”[248]

Wymieniony w definicji system informacyjny, to z kolei zorganizowany zbiór zasobów sprzętowych, programowych, osobowych, jak również organizacyjnych (proceduralnych), służący do przetwarzania oraz przesyłania informacji[249].

Inaczej niż w przypadku postanowień zawartych w Konwencji o cyberprzestępczości, przytoczona definicja nie buduje zamkniętego katalogu czynów bezprawnych, wskazując w zastępstwie dwie przesłanki, których łączne spełnienie jest niezbędne ażeby dany czyn uznać za cyberprzestępstwo:

1) czyn musi być penalizowany na mocy przepisów odrębnych - czy to krajowych, czy międzynarodowych; oraz,

---

[247] W oryginale: „*Défense et sécurité des systèmes d’information. Stratégie de la France*”. Tłumaczenie własne. Dokument dostępny na stronie internetowej pod adresem: http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011.

[248] Strategia dla Francji, s. 21. W oryginale: „*Cybercriminalité Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d’information comme moyens de réalisation d’un délit ou d’un crime, ou les ayant pour cible.*”. Tłumaczenie własne.

[249] Strategia dla Francji, s 22. W oryginale: „*Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l’information.*”. Tłumaczenie własne.

2) sieci lub systemy teleinformatyczne muszą występować w takim czynie przynajmniej w jednej z dwóch ról - jako narzędzie popełnienia przestępstwa lub jako przedmiot zamachu.

Pomimo tego, że na gruncie przywołanej definicji dopiero łączne spełnienie wyżej wymienionych przesłanek pozwala nazywać dany czyn „cyberprzestępstwem", niejasne pozostaje ścisłe określenie wzajemnego stosunku obydwu przesłanek. Czy już sama hipoteza przepisu karnego musi wyraźnie przewidywać występowanie sieci lub systemów teleinformatycznych w danym przestępstwie - czy też wystarczające jest ażeby sieci lub systemy pojawiały się dopiero w opisie faktycznym danego zdarzenia? Przyjęcie pierwszej interpretacji oznaczałoby, że cyberprzestępstwami będą wyłącznie te czyny, których sama regulacja karna już zakłada występowanie nowoczesnych technologii teleinformatycznych w jednej z ról: narzędzie lub cel zamachu. Przyjęcie drugiej interpretacji spowoduje natomiast, że cyberprzestępstwem będzie każdy czyn sankcjonowany przez dowolny przepis karny (zbiór pełny, obejmujący wszystkie przestępstwa), którego *modus operandi* dotykać będzie sieci lub systemów teleinformatycznych. Innymi słowy, pierwsza interpretacja ogranicza zakres przedmiotowy cyberprzestępstw do tych kategorii czynów, które zostały wyraźnie uregulowane, jako czyny popełniane przy użyciu lub skierowane przeciwko nowoczesnym technologiom komputerowym, podczas, gdy druga nie stawia żadnych wymogów redakcyjnych odnoszących się do sformułowań zawartych w przepisach karnych. Odwołując się do kategorii przestępstw komputerowych, zaproponowanych przez prof. A. Adamskiego, można wskazać, że pierwszy wariant obejmuje zarówno przestępstwa *stricte* komputerowe, przestępstwa, w których użycie komputera stanowi obligatoryjny element opisu prawnego czynu, jak i tzw. przestępstwa z użyciem komputera (przestępstwa „klasyczne", w których komputer występuje, jako opcjonalne narzędzie), podczas gdy drugi - wyklucza kategorię trzecią (przestępstwa z użyciem komputera), wprowadzając do zakresu pojęcia „cyberprzestępstwo" zarówno przestępstwa *stricte* komputerowe, jak i te, w których komputery występują w hipotezie przepisu karnego (*vide* uwagi zawarte w pkt 4 niniejszego paragrafu).

Komentując prezentowaną definicję, podkreślenia wymaga zatem w pierwszej kolejności fakt *szerokiego* otwarcia jej zakresu przedmiotowego. Niezależnie bowiem od przyjętej interpretacji, definicja obejmuje bardzo szeroki oraz jednocześnie niedookreślony katalog czynów, czyniąc ja równie elastyczną, co nieefektywną. Zaproponowane w definicji odwołanie do przepisów odrębnych z pewnością pozwala dopasowywać treść definiowanego

pojęcia do naturalnej ewolucji prawa, jednak z drugiej strony, nie pomaga w rekonstrukcji jego ogólnego znaczenia. Szeroki zakres definicji wiązać należy z programowym charakterem dokumentu źródłowego, którego zadaniem nie jest ustanowienie minimalnego katalogu przestępstw, które będą podlegać ściganiu - jak choćby w przypadku Konwencji o cyberprzestępczości, lecz określenie kierunków działań państwa, stanowiących odpowiedź na stale rosnące zagrożenia ze strony nowoczesnych form przestępczości komputerowej. Brak precyzji w budowie definicji doprowadza jednak do sytuacji, w której za „cyberprzestępstwo" potencjalnie na jej gruncie uznać można także zwykły akt wandalizmu skierowany np. przeciwko komputerowi wystawionemu w urzędzie, co niejako stanowi powtórzenie błędów pojawiających się w definicjach analizowanych w rozdziale pojęć, budowanych jeszcze w latach siedemdziesiątych ubiegłego stulecia.

Z punktu widzenia analizy pojęciowej, niezwykle ciekawą definicję „cyberprzestępstwa" prezentuje natomiast przyjęta w dniu 25 czerwca 2013 r. uchwałą Rady Ministrów RP „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej"[250], wprowadzająca jedną z najkrótszych, choć jednocześnie najnowocześniejszych definicji cyberprzestępstwa. Na gruncie Polityki, mianem cyberprzestępstwa określany jest:

„Czyn zabroniony popełniony w obszarze cyberprzestrzeni."

Charakterystyczną cechą przytoczonej definicji jest oczywiście jej wyraźne odwoływanie się do pojęcia cyberprzestrzeni, poruszanego w poprzedniej części rozdziału. Inaczej niż w przypadku przywołanych wcześniej definicji zagranicznych, definicja krajowa nie określa ani katalogów czynów zabronionych, które winny być penalizowane jako cyberprzestępstwa, ani szczegółowych metod działań *cyberprzestępców*, zastępując wskazane elementy odwołaniem do obszaru cyberprzestrzeni, stanowiącej cyfrową domenę przetwarzania danych. Pomimo pozornego uproszczenia definicji, zastosowane w niej odwołanie nie tylko zapewnia szeroki kontekst znaczeniowy charakteryzowanego pojęcia, ale jednocześnie pozwala także na wprowadzenie nieco mniej konwencjonalnego spojrzenia na kwestię opisu zjawiska nowoczesnej przestępczości komputerowej oraz jego form.

Stosując wcześniej zaproponowany sposób analizy przywoływanych definicji, wskazać należy, że na gruncie Polityki Ochrony Cyberprzestrzeni, cyberprzestępstwem jest każdy czyn spełniający łącznie dwie następujące przesłanki:

---

[250] Polityka Ochrony Cyberprzestrzeni RP. Pełny tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html. Należy zaznaczyć, iż dokument stanowi kontynuację wydanego w 2009 r. „Rządowego Programu Ochrony Cyberprzestrzeni RP - Założenia".

1) przedmiotowy czyn, stanowi czyn zabroniony w rozumieniu dowolnego przepisu prawnego; oraz,
2) szczególnym *miejscem* popełnienia czynu musi być cyberprzestrzeń - rozumiana nie jako kategoria geograficzna, ale nowa, logiczna domena ludzkiej działalności, podbudowywana przez szeroko rozumianą infrastrukturę teleinformatyczną, lecz nieutożsamiana z nią (cyberprzestrzeń, jako środowisko wirtualne, oderwane od substratu fizycznego).

Analizując wymienione przesłanki, jako główne kryterium zaliczania poszczególnych czynów do kategorii cyberprzestępstw, przyjęto *de facto* ocenę możliwości wystąpienia danego czynu w obszarze cyberprzestrzeni. Pojawiające się w innych definicjach kwestie oceny charakteru dóbr prawnie chronionych będących przedmiotem zamachu, roli systemów teleinformatycznych w przestępstwie, czy też opisu szczególnego rodzaju *modus operandi* sprawcy, w analizowanym przypadku straciły w efekcie swoje znaczenie na rzecz ujednoliconego odwołania do pojęcia cyberprzestrzeni. Na jego tle, uzasadnione jednak staje się zadanie następującego pytania - czy dla stwierdzenia zaistnienia tak definiowanego *cyberprzestępstwa* konieczne jest aby dany czyn w całości „zamykał się" w cyberprzestrzeni (w tym także ze swoimi skutkami), czy też wystarczające jest aby w cyberprzestrzeni wystąpiły jedynie niektóre z elementów opisujących dane przestępstwo[251]? Np. czy wprowadzenie kogoś w błąd w rozmowie telefonicznej poprzez fałszywe podanie się za osobę pracującą w dziale obsługi technicznej np. banku, skutkujące wykonaniem przez osobę oszukaną niekorzystnej operacji za pośrednictwem globalnej sieci Internet (np. przesłania hasła, czy autoryzowania przelewu *on-line*) winno być oceniane, jako cyberprzestępstwo, czy też przestępstwo „klasyczne"?

Analizując przedstawiony problem niezbędne wydaje się posiłkowe odwołanie do przepisu art. 6 § 2 Kodeksu karnego, stanowiącego, że miejscem popełnienia czynu jest miejsce działania lub zaniechania sprawcy, a także miejsce, w którym nastąpił lub jedynie miał nastąpić skutek stanowiący znamię przestępstwa. Tym samym, stwierdzić należy, że na gruncie definicji miejsca popełnienia przestępstwa, dla ukonstytuowania cyberprzestępstwa - jako przestępstwa popełnianego w cyberprzestrzeni, wystarczające jest stwierdzenie wystąpienia w obszarze domeny cyfrowej choćby jednego ze wskazanych elementów, tj. przestępnego działania, zaniechania lub skutku. W efekcie przyjętej konstrukcji, zakres

[251] *Vide* B. Fischer, Przestępstwa komputerowe i ochrona informacji. Aspekty prawno kryminalistyczne, Zakamycze, Kraków 2000, s. 25 i nast.

definicji ulega wydatnemu rozszerzeniu obejmując nie tylko typowe, bezsporne przykłady cyberprzestępstw, jak *hacking*, podmiana treści stron, czy zakłócanie poprawnego funkcjonowania systemów, ale także przypadki działań występujących *de facto* w całości poza cyberprzestrzenią. Przykładowo, wskazać można tu na zaniechanie sprawdzenia poprawnego funkcjonowania systemów teleinformatycznych, mogące sprowadzić niebezpieczeństwo dla ludzi, np. w zakresie poprawnego kierowania ruchem pojazdów. Czyn ten, choć intuicyjnie nie zalicza się do zjawiska cyberprzestępczości z uwagi na brak działania w systemach teleinformatycznych, w świetle postanowień definicji, będzie także właśnie cyberprzestępstwem.

Przyjęte w definicji w maksymalnym zakresie - z uwagi na brak wprowadzenia jakichkolwiek ograniczeń, odwołanie do cyberprzestrzeni powoduje także swoistą konkurencyjność kwalifikacji miejsca popełnienia czynu zabronionego pomiędzy przestrzenią *fizyczną*, a cyberprzestrzenią, umożliwiając przyjmowanie podwójnej kwalifikacji dla jednego czynu (np. w sytuacji gdy działanie przestępne występuje w świecie fizycznym, zaś skutek pojawia się w cyberprzestrzeni). Rozwiązanie takie, choć nie ułatwia definiowania przestępczości cyberprzestrzeni, wydatnie zwraca uwagę na fakt ustawicznego przeplatania się współczesnych społeczeństw z nowoczesnymi technologiami teleinformatycznymi, w tym technologiami cyberprzestrzeni.

Oceniając definicję cyberprzestępstwa proponowaną na gruncie krajowej Polityki Ochrony Cyberprzestrzeni, należy stwierdzić, iż pomimo jej szerokiego zakresu przedmiotowego, definicja ta wyznacza nowoczesny kierunek utożsamiania cyberprzestępczości z przestępczością popełnianą w cyberprzestrzeni, niezależnie od jej form oraz szczegółowych metod działania sprawcy. Przyjęte założenie pozwala uniknąć tworzenia specyficznych katalogów cyberprzestępstw, stawiając swoisty znak równości pomiędzy przestępczością „klasyczną" a cyberprzestępczością, z jednoczesnym wprowadzeniem kryterium miejsca popełnienia przestępstwa, jako definiującym istotę cyberprzestępczości.

Pozostając w obszarze polskich regulacji krajowych - choć rozwiązanie to aktualnie przestało już obowiązywać, niezbędne jest również wskazanie przepisów rozporządzenia Ministra Sprawiedliwości z dnia 20 kwietnia 2004 r. w sprawie wzoru europejskiego nakazu aresztowania[252], w którym to wzorze uwzględniona została kategoria „cyberprzestępczości", pojawiając się w część E.1 nakazu. Wskazana część dotyczy określenia czynów stanowiących podstawę wydania nakazu. Analizowana kategoria „cyberprzestępczości" wprowadzona

[252] Dz. U. Nr 73, poz. 664.

została do wzoru z pominięciem jakiegokolwiek przybliżenia, czy zdefiniowania, pozostawiając tym samym ocenę kwalifikacji czynu jako cyberprzestępstwa, do wyłącznej gestii osoby sporządzającej nakaz. Z punktu widzenia zasad techniki legislacyjnej, dodać trzeba, że ewentualna definicja powinna zostać wprowadzona na gruncie ustawy, a nie aktu wykonawczego - w szczególności zaś rozporządzenia, które ma określić jedynie wzór dokumentu. W reakcji na powyższą sytuację, zaledwie dziesięć dni po podpisaniu rozporządzenia, w dniu 30 kwietnia 2004 wydane zostało obwieszczenie Prezesa Rady Ministrów o sprostowaniu błędu[253], zawierające dodatkowe pouczenie dotyczące wypełniania wzoru. W pouczeniu tym wskazano m. in., że:

> „czyny w zakresie cyberprzestępczości - oznaczają czyny przeciwko ochronie danych gromadzonych, przechowywanych, przetwarzanych lub przekazywanych w systemie informatycznym".

W efekcie przyjęcia powyższego pouczenia, stworzono nową kategorię pojęciową „czynów w zakresie cyberprzestępczości", którą objęte zostały *de facto* wszelkie czyny skierowane przeciwko „ochronie danych". Pomijając już fakt przekroczenia granic delegacji ustawowej, przyjęta definicja nie tylko ukształtowana została w sposób zbyt szeroki, obejmując czyny polegające na działaniach dokonywanych w ogóle poza cyberprzestrzenią (np. akt wandalizmu wobec komputera), ale w sposób niejasny, wskazywała także - opisując przedmiot analizowanej tu kategorii przestępczości, nie tyle na same dane, co na ich ochronę. W świetle przytoczonej definicji, czynem w zakresie cyberprzestępczości nie był zatem czyn, który naruszał dane, lecz czyn, który naruszał ochronę tychże danych. Brak sprecyzowania, o jaką ochronę chodziło, nakazywał w tej sytuacji stosować domniemanie prowadzące do przepisów Kodeksu karnego, pozostawiając jednak wątpliwość, czy wyrażenie „ochrona" należy rozumieć w sensie wyłącznie prawnym, czy też technicznym. Co gorsza, literalne brzmienie przepisu, który odniesiony został do pojedynczego systemu informatycznego, uprawnia tezę, że do czynów w zakresie cyberprzestępczości nie zaliczają się czyny dokonywane w sieciach, to jest „pomiędzy" systemami, np. podsłuchiwanie transmisji danych. Z uwagi na ograniczone zastosowanie przepisów rozporządzenia, komentowana definicja nie zyskała rozgłosu, będąc najczęściej pomijaną w rozważaniach na temat przestępczości cyberprzestrzeni. Co więcej, aktualnie, rozporządzenie utraciło moc obowiązującą, po tym jak zostało uchylone przez nowe rozporządzenie w sprawie wzoru europejskiego nakazu aresztowania[254]. Obowiązujący dokument nie powtórzył pojęcia

[253] Dz. U. Nr 99, poz. 1004.
[254] Dz. U. z 2012 r., poz. 266.

„cyberprzestępczość”, zastępując je „przestępstwem przeciwko ochronie danych gromadzonych, przechowywanych, przetwarzanych lub przekazywanych w systemie informatycznym”, powtarzając tym samym opisane wyżej błędy definicyjne oraz zakresowe.

Przechodząc na grunt literatury prawniczej, zauważyć można, że pojęciem „cyberprzestępstwa” posługuje się także coraz więcej nowych opracowań przedmiotu, w szczególności zaś opracowań amerykańskich[255]. Pojęciem tym posługuje się także Federalne Biuro Śledcze USA (FBI), wykorzystując je w swoich biuletynach informacyjnych publikowanych na oficjalnej stronie internetowej agencji. Po części w kontekście Konwencji o cyberprzestępczości, wyrażenie „cyberprzestępstwo” wykorzystywane jest także w piśmiennictwie europejskim, zdobywając jednak coraz większą popularność wśród autorów - w tym też autorów polskich. Pośród opracowań krajowych, pojęciem tym w szczególności posłużył się prof. A. Adamski w swoim artykule zatytułowanym „Cyberprzestępczość - aspekty prawne i kryminologiczne”, który to tekst ukazał się w 2005 r.[256]. Zachowując przekrojowy charakter artykułu, jego autor zaprezentował na jego łamach systematykę cyberprzestępczości, stanowiącą swoiste rozwinięcie koncepcji przedstawionych wcześniej w „Prawie karnym komputerowym” (2000 r.). Na potrzeby analizy, cyberprzestępczość podzielona została w artykule na cztery robocze kategorie:

1) przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych (np. nieuprawniony dostęp do systemu, podsłuchiwanie transmisji danych, czy też zakłócanie funkcjonowania systemów);
2) przestępstwa przeciwko dostępowi warunkowemu do usług informacyjnych (np. nieuprawniony dostęp do płatnej, kodowanej telewizji);
3) przestępstwa związane z używaniem komputerów (np. oszustwo komputerowe, czy fałszerstwo komputerowe); oraz,
4) przestępstwa związane z rozpowszechnianiem lub przesyłaniem określonych rodzajów informacji (np. propagowanie treści rasistowskich, pornografii dziecięcej, czy choćby rozsyłanie niezamówionych informacji handlowych - tzw. *spam*).

Odwołując się do systematyki przyjętej w „Prawie karnym komputerowym” (szeroko opisanej w pkt 4. paragrafu), kategorię pierwszą przyrównać można do przestępstw *stricte* komputerowych, podczas gdy kategorie 3 i 4 przecinają się zakresowo z „przestępstwami z użyciem komputera” (przestępstwa klasyczne, popełniane przy wykorzystaniu komputera)

[255] Np. M. Cross, D. Littlejohn Shinder, *Scene of the Cybercrime*, Syngress 2008, czy A. Reyes, *Cyber Crime Investigations*, Elsevier, USA, 2007 - by wskazać jedne z najczęściej cytowanych pozycji.
[256] A. Adamski, Cyberprzestępczość... op. cit., s. 51 i nast.

oraz „przestępstwami komputerowymi w ujęciu szerokim" (przestępstwa, odnośnie których przepis karny przewiduje szczególny *modus operandi* sprawcy, zakładający obligatoryjne wykorzystanie komputera lub sieci). Kategoria 2. obejmująca przestępstwa przeciwko warunkowemu dostępowi do informacji - zawężając analizę wyłącznie do obszaru cyberprzestrzeni, wydaje się natomiast stanowić szczególną podgrupę przestępstw kierowanych przeciwko poufności, integralności i dostępności danych i systemów komputerowych (kategoria 1.), zaliczając się tym samym ponownie do przestępstw *stricte* komputerowych.

7. Pojęcia wspomagające: „incydent" oraz „atak".

Obok przybliżonych pojęć o charakterze *quasi*-karnistycznym, skupiających się głównie na ujęciu nowoczesnej przestępczości komputerowej, jako zjawisku podlegającym określonej sankcji prawnej, w obszarze szeroko rozumianego bezpieczeństwa teleinformatycznego stosuje się także określenia o konotacji mniej formalnej, zaś bardziej technicznej. Pojęcia te pozwalają stawiać akcent nie tyle na prawnie zdefiniowanym przestępstwie, czy przesłankach jego wystąpienia, co faktycznie zaistniałym zdarzeniu o określonych cechach technicznych, w szczególności odnoszących się do *modus operandi* sprawcy. Na szczególne uwzględnienie zasługują tu określenia „incydent" oraz „atak".

Pojęcie incydentu spotkać można w wielu formach. W najogólniejszym znaczeniu mówi się o „incydencie bezpieczeństwa", jak zdarzeniu naruszającym określony stan faktyczny lub projektowany, który uznawany jest za pożądany, jako bezpieczny. W swojej czystej postaci, pojęcie to stosowane jest przede wszystkim na gruncie teorii, jak i praktyki zarządzania bezpieczeństwem. W obszarze teleinformatyki głównie wykorzystywane są zaś pojęcia „incydentu bezpieczeństwa komputerowego", „incydentu cyber bezpieczeństwa", jak również „incydentu bezpieczeństwa teleinformatycznego".

Pierwsze z wymienionych sformułowań - „incydent bezpieczeństwa komputerowego", zdefiniowane zostało w szczególności przez amerykańską rządową agendę standaryzacyjną NIST - *National Institute of Standards and Technology*, funkcjonującą w ramach ministerstwa handlu USA (*Department of Commerce*)[257]. W opublikowanym przez NIST w 2008 r. „Przewodniku Obsługi Incydentów Bezpieczeństwa Komputerowego" (Publikacja Specjalna 800-61)[258], pojęciu temu nadano następujące znaczenie:

[257] Więcej na temat NIST na stronie internetowej pod adresem: http://itlaw.wikia.com/wiki/National_Institute_of_Standards_and_Technology, a także oficjalnej stronie internetowej instytutu pod adresem: www.nist.gov.
[258] Tytuł oryginalny: „*Computer Security Incident Handling Guide*". Tłumaczenie własne. Pełny dokument

„*Incydentem bezpieczeństwa komputerowego* jest naruszenie lub rzeczywista groźba naruszenia przyjętej polityki bezpieczeństwa komputerowego, polityki określającej zasady dozwolonego użytku lub standardowych praktyk bezpieczeństwa."[259].

Zgodnie z przyjętym brzmieniem definicji, wskazane wyżej pojęcie zostało odniesione do wszelkich działań naruszających szeroko rozumiane bezpieczeństwo komputerowe, co w szczególności oznacza wykroczenie poza zakres czynów podlegających kwalifikacji karnej, czy nawet szerzej - jakiejkolwiek ocenie prawnej. Incydentem nazwane zostały wszelkie naruszenia nie tylko zasad pracy przyjętych w skonkretyzowanym systemie, ale również standardowych praktyk stosowanych w zakresie zabezpieczania systemów oraz sieci. Jako przykłady incydentów, Przewodnik wskazuje: incydent odmowy dostępu, polegający na zaburzeniu poprawnego funkcjonowania systemu poprzez wywołanie jego nadmiernego obciążenia; incydent wprowadzenia do systemu złośliwego oprogramowania powodującego wykonywanie niechcianych operacji; incydent nieuprawnionego dostępu do systemu; oraz incydent niedopuszczalnego wykorzystywania funkcji systemu, np. poprzez bezprawne kopiowanie i wynoszenie poza system danych podlegających ochronie. Zarówno przytoczona definicja, jak i przykładowy katalog incydentów nie przesądzają jednoznacznie, czy incydentem powinny być nazywane także zdarzenia faktyczne nie będące wynikiem bezpośredniego działania człowieka, które nie odnoszą się bezpośrednio do wymogów bezpieczeństwa stawianych dla danego systemu - np. związane ze stwierdzeniem występowania w systemie luki bezpieczeństwa. Wiele z takich luk wynikać może bowiem z samego zastosowania określonego systemu operacyjnego posiadającego ukryte wady, które w praktyce ujawniają się często nawet po kilku latach od rynkowej premiery oprogramowania. Przyjąć należy, że szczegółowe rozwiązania w tym zakresie pozostawione zostały jednak politykom bezpieczeństwa poszczególnych systemów, w których to politykach możliwe jest dalsze dookreślenie katalogu naruszeń sprzeciwiających się przyjętym zasadom bezpieczeństwa. Pojęcie „incydentu bezpieczeństwa komputerowego" wykorzystywane jest szeroko między innymi przez tworzące globalną siatkę zespoły reagowania na incydenty, funkcjonujące najczęściej pod zastrzeżonymi nazwami CSIRT - *Computer Security Incident Response Team*, jak również CERT - *Computer Emergency Response Team*[260].

---

dostępny na stronie internetowej pod adresem: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

[259] W oryginale: „*A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices*". Tłumaczenie własne. Przewodnik obsługi incydentów bezpieczeństwa komputerowego, część 2-1.

[260] Więcej na temat historii stosowanych nazw na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Computer_emergency_response_team.

Przykładowa definicja drugiego z wymienionych pojęć - „incydentu cyber bezpieczeństwa”, zamieszczona została w pochodzącym z 2009 r. „Słowniku wyrażeń wykorzystywanych w standardach niezawodności”[261]. Publikacja ta przygotowana została przez NERC - *North American Electric Reliability Corporation*, będący amerykańską pozarządową organizacją standaryzacyjną pracującą głównie w obszarach bezpieczeństwa energetycznego oraz ochrony infrastruktury krytycznej. Słownik zdefiniował incydent cyber bezpieczeństwa, jako:

> „Każde złośliwe działanie lub zdarzenie, które przełamuje lub usiłuje przełamać zastosowane środki ochrony fizycznej lub elektronicznej cyber zasobu o charakterze krytycznym z punktu widzenia funkcjonowania państwa, lub zakłóca lub usiłuje zakłócić poprawne działanie takiego zasobu.” [262].

Nieco szerzej, niż w przypadku przywołanej wcześniej definicji incydentu bezpieczeństwa komputerowego, pojęcie „incydentu cyber bezpieczeństwa” odniesione zostało wprost do wszelkich działań oraz zdarzeń faktycznych naruszających szeroko rozumiane bezpieczeństwo. Podobnie jak poprzednio, dla przeprowadzenia kwalifikacji zdarzenia złośliwego, jako incydentu, bez znaczenia uznany został fakt, czy dane naruszenie bezpieczeństwa stanowi efekt dokonania czynu bezprawnego, czy też w ogóle nie podlega jakimkolwiek ocenom prawnym. Incydentem cyber bezpieczeństwa staje się bowiem każde zdarzenie, które w sposób obiektywny wpływa na samo bezpieczeństwo lub też poprawne funkcjonowanie określonego w definicji zasobu, obejmując w efekcie także wewnętrzne wady samego systemu oraz ukryte w nim luki bezpieczeństwa. Z uwagi na przeznaczenie definicji, odnoszącej się do obszaru ochrony infrastruktury krytycznej, zakres przedmiotowy incydentu cyber bezpieczeństwa ograniczony został do systemów kluczowych dla poprawnego funkcjonowania państwa. Do systemów takich zaliczyć należy przede wszystkim systemy wspomagające lub obsługujące elementy infrastruktury krytycznej odpowiedzialne za dostarczanie energii, wody, ochronę zdrowia, a także zapewnianie bezpieczeństwa wewnętrznego państwa, w tym bezpieczeństwa ekonomicznego.

Ostatecznie, trzecie z wymienionych określeń - „incydent bezpieczeństwa teleinformatycznego”, należy do zasobu polskiego języka prawnego, występując na gruncie obowiązujących regulacji z zakresu ochrony informacji niejawnych. Wydane w dniu 20 lipca

---

[261] W oryginale: „*Glossary of Terms Used in Reliability Standards*”. Przywołano za wpisem encyklopedycznym pochodzącym ze strony internetowej pod adresem: http://itlaw.wikia.com/wiki/Cyber_security_incident.

[262] W oryginale: „*Any malicious act or event that: Compromises, or attempts to compromise, the electronic or physical security perimeter of a critical cyber asset, or Disrupts or attempts to disrupt the operation of a critical cyber asset.*”. Tłumaczenie własne. Powtórzono za wpisem encyklopedycznym pochodzącym ze strony internetowej pod adresem: http://itlaw.wikia.com/wiki/Cyber_security_incident.

2011 r. rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego[263] - stanowiące wykonanie delegacji zawartej w przepisie rozdziału 8. ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[264], zatytułowanego „Bezpieczeństwo teleinformatyczne", zdefiniowało w § 2 pkt 3 pojęcie „incydentu bezpieczeństwa teleinformatycznego", jako:

> „takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności".

Porównując kolejne definicje incydentów bezpieczeństwa, przytoczona tu definicja z rozporządzenia w sposób najbardziej jednoznaczny odrywa pojęcie „incydentu" od skonkretyzowanego działania ewentualnego sprawcy naruszenia bezpieczeństwa. Na gruncie przepisu, incydent został wprost utożsamiony ze „zdarzeniem" obejmując tym samym zarówno wszelkie działania, jak i zaniechania osób, jak też dowolne okoliczności faktyczne wpływające negatywnie na bezpieczeństwo danych przetwarzanych w systemach teleinformatycznych. W efekcie, w świetle definicji krajowej już nawet nie tylko podatności systemu, czy występujące w nim luki bezpieczeństwa mogą być kwalifikowane jako incydenty, lecz także np. występujący faktycznie brak zasilania, przekreślający dostępność informacji, czyli właściwość określającą, że dany zasób systemu możliwy jest do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie[265]. Podobnie, jak w przypadku wcześniej analizowanych definicji, także i tu incydent został oderwany od dodatkowych kwalifikacji prawnych, nabierając czysto faktycznej konotacji. W szczególności, pojęcie incydentu bezpieczeństwa teleinformatycznego nie zostało odniesione do zdarzeń podlegających ocenie prawnokarnej, choć oczywiście wiele z potencjalnych incydentów będzie mogło stanowić efekt popełnienia przestępstwa i podlegać ściganiu ze strony wymiaru sprawiedliwości. Choć przywołana definicja została ograniczona przedmiotowo do bezpieczeństwa informacji niejawnych – co stanowi bezpośrednie odzwierciedlenie obszaru regulacyjnego rozporządzenia, na potrzeby prowadzonej analizy pojęciowej, jej ogólną treść można odnosić do wszelkich informacji przetwarzanych w postaci elektronicznej.

Uzupełniająco, warto wskazać, że pojęciem incydentu posłużono się również na gruncie przepisów innego krajowego aktu wykonawczego - mianowicie rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności,

---

[263] Dz. U. Nr 159, poz. 948.
[264] Dz. U. z 2016 r., poz 1167, z późn. zm.
[265] Na podstawie § 2 pkt 1 przytaczanego rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.

minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[266], gdzie wyrażenie to pojawiło się w kontekście naruszeń bezpieczeństwa informacji. Wskazane rozporządzenie nie wprowadziło jednak definicji analizowanego pojęcia.

Należy zaznaczyć, iż zupełnie niekonsekwentnie - w kontekście powyższego przybliżenia krajowej siatki terminologicznej, w wydanej w Polsce w 2013 r. Polityce Ochrony Cyberprzestrzeni RP zastosowane zostało pojęcie „incydentu związanego z bezpieczeństwem informacji" - zdefiniowane, jako:

> „pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji - (wg norm serii PN-ISO/IEC 27000)"[267].

Choć rdzeń pojęcia - to jest zdarzenie lub seria zdarzeń istotnych w kontekście bezpieczeństwa informacji, pozostał zbieżny z definicjami prezentowanymi powyżej, z niewyjaśnionych przyczyn w opisywanej definicji, przyjętej w Polityce, za główną przesłankę kwalifikacji wydarzenia, jako incydentu przyjęto nieprecyzyjne pojęcie „zakłócenia działań biznesowych". Pojęcie to należy odbierać, jako odnoszące się do sfery komercyjnej, nie zaś bezpieczeństwa cyberprzestrzeni, jako samodzielnej wartości prawnej. Zastosowany tu zabieg legislacyjny trzeba w tej sytuacji oceniać negatywnie, jako wprowadzający zamieszanie terminologiczne oraz niezwykle niejasne odwołanie do wartości biznesowych (można dodać - oportunistycznych).

Istotnie różniące się znaczeniowo od pojęcia „incydent" jest natomiast określenie „atak" („cyber atak"), odnoszące się do skonkretyzowanego działania sprawcy naruszenia bezpieczeństwa systemu teleinformatycznego. W przypadku ataku nie można zatem mówić o dowolnym zdarzeniu naruszającym przyjęte zasady funkcjonowania danego systemu, bowiem pojęcie to odwołuje się do bezprawnego, umyślnego działania o *stricte* ofensywnej treści. Warto nadmienić, że pojęcie cyber ataku wywodzi się wprost z nowoczesnej doktryny wojennej USA stanowiąc jeden z elementów tzw. cyber wojny (z ang. *cyberwarfare*[268]). W swoich kontekstach występowania, wyrażenie „atak" najczęściej nabiera konotacji technicznej, łącząc się z określeniem szczegółowego *modus operandi* sprawcy - przykładowo

---

[266] Dz. U. Nr 0, poz. 526.

[267] Polityka Ochrony Cyberprzestrzeni RP. Pełny tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html.

[268] Więcej na ten temat na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Cyberwarfare.

mówi się o atakach *hackerskich*, atakach odmowy dostępu, atakach typu *man-in-the-middle,* czy wreszcie atakach słownikowych na stosowane w systemach hasła. Sformułowania te odnoszą się do metod popełniania przestępstw w cyberprzestrzeni.

Przykładowa definicja cyber ataku zaprezentowana została na gruncie przytaczanej w poprzedniej części rozdziału rządowej Strategii Cyber Bezpieczeństwa dla Niemiec[269], gdzie przewidziano, że:

> „Cyber atakiem jest każdy atak informatyczny występujący w cyberprzestrzeni skierowany przeciwko jednemu lub wielu systemom teleinformatycznym, nakierowany na naruszenie bezpieczeństwa teleinformatycznego. Cele bezpieczeństwa, poufność, integralność oraz dostępność mogą być naruszane łącznie lub indywidualnie. Cyber ataki przeciwko poufności systemu, które są wykonywane lub kierowane przez obce służby wywiadowcze, nazywane są cyber szpiegostwem. Cyber ataki przeciwko integralności oraz dostępności systemów, określane są zaś mianem cyber sabotażu.” [270].

Zgodnie z wcześniejszą uwagą, atakiem określono wyłącznie działania nakierowane specyficznie przeciwko bezpieczeństwu systemów teleinformatycznych oraz przetwarzanych w tych systemach danych, charakteryzowanemu standardowo przez pryzmat poufności, integralności oraz dostępności. Prezentując kontekst występowania pojęcia, w treści Strategii jej twórcy odwołują się do nowych, złożonych ataków, ataków z ukrycia oraz różnych form ataków - które to wyrażenia stanowią odniesienie do opisu metod przeprowadzania ataków. W kontekście tym pojawia się w strategii także przywołanie oprogramowania złośliwego, będącego jednym z narzędzi do przeprowadzenia cyber ataków. Należy bowiem zaznaczyć, że atak może zostać wykonany nie tylko w sposób bezpośredni, wymagający działania sprawcy w czasie występowania samego ataku, ale także zautomatyzowany - np. z wykorzystaniem odpowiednio przygotowanego w tym celu oprogramowania lub też sieci tzw. komputerów *zombie* (sieci Botnet).

Za sprawą tytułu Decyzji Ramowej Rady z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[271], pojęcie „ataku” jest także pojęciem języka prawnego,

---

[269] W oryginale: „*Cyber Security Strategy for Germany*.”. Dokument w wersji anglojęzycznej dostępny na stronie internetowej pod adresem: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.

[270] W oryginale: „*A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage*.”. Strategia Cyber Bezpieczeństwa dla Niemiec, s. 9. Tłumaczenie własne.

[271] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW. Pełen tekst dokumentu dostępny jest na stronie internetowej pod

występując w jednym z aktów normatywnych Unii Europejskiej. Przywołany dokument nie wprowadził jednak żadnej definicji tego wyrażenia, ograniczając jego występowanie do tytułu oraz preambuły aktu. Analizując kontekst, w jakim na gruncie Decyzji pojawia się określenie „atak”, stwierdzić można natomiast, że, rozumienie wskazanego pojęcia nie odbiega od tego zaprezentowanego wyżej w odniesieniu do Strategii Niemiec. Przykładowo, pkt 14 Preambuły Decyzji, stanowi, że: „Istnieje potrzeba ustanowienia przez Państwa Członkowskie sankcji za ataki na systemy informatyczne.”. Wyrażenie „atak” ponownie zatem zostało odniesione do czynności faktycznych, służących do określania znamion poszczególnych przestępstw.

Przyjęta w Polsce w 2013 r. - jako najpóźniejsza z prezentowanych tu dokumentów programowych, Polityka Ochrony Cyberprzestrzeni RP wprowadziła do polskiego obrotu prawnego także krajową definicję pojęcia „cyberatak”, które zostało scharakteryzowane, jako:

„celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni”[272].

Tak, jak w przypadku poprzednich rozważań - analizowane ujęcie definicyjne odniesiono do działań nakierowywanych na naruszenie bezpieczeństwa cyberprzestrzeni, pozostawiając charakter samych działań bez bliższego doprecyzowywania. W definicji krajowej podkreślono natomiast celowy charakter ataku, wykluczając tym samym z desygnatów opisywanego pojęcia działania niezamierzone. Jako uwagę krytyczną należy w tym miejscu wskazać na zasadność zastąpienia użytego w definicji wyrażenia „celowe” zwrotem kodeksowym odnoszącym się do pojęcia winy.

PODSUMOWANIE

Zawarta w § 1 niniejszego rozdziału analiza wybranych definicji „cyberprzestrzeni” - będących definicjami pochodzącymi nie tylko z różnych systemów prawnych, ale także z aktów nienormatywnych, w pełni uzasadnia stwierdzenie, że termin ten jest w istocie złożony oraz wieloaspektowy. Jego pełne zrozumienie wymaga podjęcia rozważań na wielu płaszczyznach, w tym zarówno prawnej, informatycznej, jak i nawet socjologicznej. Co warte zaznaczenia – wskazane płaszczyzny na gruncie omawianych definicji wzajemnie się przenikają oraz uzupełniają do tego stopnia, że ich wtórny rozdział wydaje się wypaczać

---

adresem: http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:PL:PDF.

[272] Polityka Ochrony Cyberprzestrzeni RP. Pełny tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html.

poprawne rozumienie omawianego pojęcia. Podsumowując zatem powtarzające się w definicjach fizyczne elementy cyberprzestrzeni, wskazać należy na następujący katalog:

- podstawy technologiczne: szeroko rozumiany sprzęt, w skład, którego wchodzą elementy sieci telekomunikacyjnych - centrale, łącza, infrastruktura sieciowa; podłączone do nich komputery oraz wszelkie inne urządzenia przetwarzające dane w postaci cyfrowej; oraz oprogramowanie, zarówno to instalowane przez użytkowników (aplikacje), jak i tzw. *firmware* stanowiący oprogramowanie wewnętrzne urządzeń, podkreślenia wymaga stwierdzenie, iż głównym filarem cyberprzestrzeni są aktualnie rozległe sieci teleinformatyczne, przede wszystkim zaś Internet,
- przetwarzane w systemach dane w postaci elektronicznej, stanowiące cyfrowe odzwierciedlenie informacji, dóbr prawnych, usług oraz treść szeroko rozumianych działań dokonywanych w sieciach,
- użytkownicy, którzy choć oczywiście nie stanowią budulca cyberprzestrzeni, kształtują jej niezbędny element, bez którego cyberprzestrzeń nie mogłaby istnieć; to bowiem technologie istnieją dla ludzi, a nie odwrotnie,

Wymienione elementy warunkują natomiast następujące cechy cyberprzestrzeni, również pojawiające się w przybliżonych definicjach:

- cyberprzestrzeń to twór sztuczny, w którym *per se* nie funkcjonują prawa fizyki znane z otaczającej nas rzeczywistości,
- poruszanie się po cyberprzestrzeni możliwe jest wyłącznie za pośrednictwem nowoczesnych urządzeń teleinformatycznych,
- opisana powyżej infrastruktura tworzy nowe środowisko, cyfrową przestrzeń, stanowiącą forum aktywności społecznej; środowisko to odrywa się od samej infrastruktury tworząc spójny obszar logiczny, zbudowany wspólnie z zasobów rozsianych po całym globie; środowiska tego nie można rozumieć jednak w sposób analogiczny, jak sfer lądu, morza i powietrza,
- cyberprzestrzeń, choć tworzona przez technologie, istnieje *ponad* nimi i nie może być utożsamiana z warstwą technologiczną,
- tworząc domenę jakościowo różną od świata fizycznego, cyberprzestrzeń wymaga wytworzenia nowych reguł prawnych oraz zwyczajów rządzących w jej obszarze – nie wszystkie bowiem regulacje prawne odnoszące się do działań *fizycznych* mogą w sposób prosty zostać odzwierciedlone w rzeczywistości *cyfrowej*,

- cyberprzestrzeń, z uwagi na swoją budowę przybiera globalny zasięg, co więcej łączy sieci zarówno prywatne, jak i państwowe,
- jedną z podstawowych cech cyfrowej domeny jest jej rozszerzalność, rozumiana jako niczym nie ograniczona możliwość ustawicznego rozbudowywanie zasobów cyberprzestrzeni oraz włączania do jej obszaru nowych technologii oraz urządzeń,
- wskazane powyżej cechy: globalny zasięg, łączenie sieci prywatnych i państwowych, tworzenie nowej sfery oderwanej logicznie od podbudowującej ją infrastruktury zarysowują wydatny problem w zwalczaniu nowoczesnych form przestępczości - brak jednoznacznej jurysdykcji,
- transparentność technologiczna, łatwość uczestnictwa – posługiwanie się komputerami, poruszanie po sieci, w szczególności Internecie, nie wymaga dziś już znajomości tajników informatyki,
- interaktywność – cyberprzestrzeń nie stanowi medium jednostronnego, poddaje się kształtowaniu użytkowników; na poziomie technologicznym interaktywność należy rozumieć także, jako możliwość wykorzystywania infrastruktury, która nie stanowi naszej własności oraz znajduje się często na drugim końcu świata – proste otwarcie strony Internetowej niejednokrotnie wiąże się z uruchomieniem całej sieci połączeń infrastrukturalnych,
- szeroki dostęp oraz generalna bezpłatność za dostęp do zasobów sieci powodują mieszanie się kultur oraz języków, wymianę informacji i poglądów a w efekcie budowanie nowego ponadnarodowego społeczeństwa,
- rosnący udział cyberprzestrzeni w codziennym życiu stał się przyczyną dla przenikania się działań dokonywanych w cyberprzestrzeni z konsekwencjami występującymi w realnym świecie; aktualnie funkcjonalnie obie te sfery są już trwale, wzajemnie połączone,
- uzależnienie nowoczesnych form handlu, reklamy, ale także krytycznych usług świadczonych przez państwa na rzecz swoich obywateli, uzależniające w coraz większej mierze poprawne funkcjonowanie społeczeństw od niezaburzonego działania cyberprzestrzeni, spowodowały ogromną rolę nowej domeny tak dla poszczególnych ludzi, ekonomii, jak i bezpieczeństwa wewnętrznego oraz międzynarodowego,
- globalność cyberprzestrzeni, którą należy postrzegać jako obszar spójny, stanowiący wielką całość, oznacza, że systemy teleinformatyczne odseparowane od rozległych

sieci – w praktyce przede wszystkim od Internetu, nie stanowią elementu cyberprzestrzeni, budują zaś jej nowy, niezależny skrawek.

Cyberprzestrzeń zatem to nie tylko suma fizycznych składników – systemów, sieci, oprogramowania oraz przetwarzanych w nich informacji. To nie proste odwołanie do Internetu - choć niewątpliwie to właśnie Internet stanowi dzisiaj ilościowo najistotniejszy składnik cyberprzestrzeni, mieszcząc się w każdej omawianej definicji oraz będąc wymieniany wprost w części z nich. Cyberprzestrzeń to wreszcie nie suma operacji wykonywanych przez użytkowników w sieciach. Istotę cyberprzestrzeni stanowi bowiem koncepcja powołania do życia swojego rodzaju równoległego środowiska stanowiącego nowy wymiar dla ludzkich działań. Wymiar ten, z uwagi na sposób budowy, stanowi jednak obszar wymykający się opisowi przy użyciu typowych, fizycznych miar, zatem nie poddaje się prostemu podziałowi geograficznemu pomiędzy państwa.

Cyberprzestrzeń bowiem z uwagi na swoją budowę posiada unikalną fizykę, w której zamiast atomów istnieją bity zaś środowisko naturalne zastąpione jest środowiskiem programowym. Cyfrowy zapis danych stanowi tu nie tylko sposób odzwierciedlania dóbr prawnych, ale jest także wyłącznym budulcem dla niektórych z nich, nieistniejących w ogóle w innej postaci – np. informacji przetwarzanych wyłącznie w sieciach komputerowych. Tych specyficznych praw fizyki doświadczyć można oczywiście wyłącznie za pośrednictwem systemów teleinformatycznych. Z uwagi jednak na powszechną dostępność nowoczesnych technologii komputerowych oraz omalże nieograniczony zasięg Internetu, użytkownikami tego tylko składnika cyberprzestrzeni są dziś już ponad dwa miliardy ludzi, którzy codziennie goszczą oraz działają w cyfrowej domenie za pośrednictwem 5 miliardów podłączonych do Internetu urządzeń[273]. Brak stosownych definicji oraz rozwiązań prawnych, które po wprowadzeniu do ustaw karnych pozwoliłyby uwzględniać w toczących się procesach specyfikę cyberprzestrzeni, należy zatem uznać jako wyraz nienadążania prawa za postępem technologicznym.

Przechodząc do podsumowania zawartej w § 2 rozdziału prezentacji pojęć odnoszących się do zjawiska przestępczości w cyberprzestrzeni, w pierwszej kolejności warto zwrócić uwagę na chronologię występowania poszczególnych określeń. Zestawienie takie umożliwia nie tylko dokonanie syntetycznego ujęcia zaprezentowanych w rozdziale dokumentów oraz występujących na ich gruncie pojęć, ale pozwala także na przeanalizowanie

[273] Strategia Cyberbezpieczeństwa Zjednoczonego Królestwa, Ochrona oraz promocja Zjednoczonego Królestwa w cyfrowym świecie, s. 10.

występujących trendów rozwoju stosowanej siatki pojęciowej. Pełne zestawienie dokumentów oraz wyrażeń prezentuje poniższa tabela.

Tabela porównawcza - ujęcie chronologiczne występowania analizowanych pojęć.

Lp.	Rok wydania:	Rodzaj oraz oryginalny tytuł dokumentu źródłowego:	Pojęcie stosowane jako centralne,	
			w oryginale:	w tłumaczeniu:
1.	1976	**Opracowanie naukowe**: D. B. Parker, *Crime by Computer*.	**Computer abuse**	**Nadużycie komputerowe**
2.	1979	**Rządowy podręcznik USA**: *Computer Crime: Criminal Justice Resource Manual.*	**Computer-related crime**	**Przestępstwo związane z komputerem**
3.	1986	**Raport OECD**: *Computer-related crime: Analysis of legal policy*.	**Computer abuse**	**Nadużycie komputerowe**
4.	1986	**Ustawa USA**: *Computer Fraud and Abuse Act.*	**Computer abuse**	**Nadużycie komputerowe**
5.	1989	**Zalecenie Komitetu Ministrów Rady Europy**: *Recommendation No. R (89)9 on computer-related crime* [...].	**Computer-related crime**	**Przestępstwo związane z komputerem**
6.	1990	**Ustawa Zjednoczonego Królestwa**: *Computer Misuse Act 1990.*	**Computer misuse**	**Bezprawne użycie komputera**
7.	1990	**Rezolucja VIII. Kongresu ONZ**: *Computer-related crime.*	**Computer-related crime**	**Przestępstwo związane z komputerem**
8.	1994	**Podręcznik ONZ**: *United Nations Manual on the prevention and control of computer-related crime.*	**Computer crime = Computer-related crime**	**Przestępstwo komputerowe = Przestępstwo związane z komputerem**

9.	**1995**	**Zalecenie Komitetu Ministrów Rady Europy**: *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law* [...].	**Offence connected with Information Technology**	**Przestępstwo powiązane z technologią informacyjną**
10.	**2000**	**Opracowanie naukowe**: A. Adamski, *Prawo karne komputerowe*.	**Przestępstwo komputerowe**	
11.	**2001**	**Konwencja Rady Europy**: *Convention on Cybercrime*.	**Cybercrime**	**Cyberprzestępstwo**
12.	**2003**	**Rządowy program USA:** *The National Strategy to Secure Cyberspace*.	**Cybercrime**	**Cyberprzestępstwo**
13.	**2009**	**Rządowy program Polski:** Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009 - 2011.	**Cyberprzestępstwo**	
14.	**2009**	**Rządowy program Zjednoczonego Królestwa:** *Cyber Security Strategy of the United Kingdom* [...].	**Cyber crime**	**Cyber przestępstwo**
15.	**2011**	**Rządowy program Zjednoczonego Królestwa:** The UK Cyber Security Strategy [...].	**Cyber crime**	**Cyber przestępstwo**
16.	**2011**	**Rządowy program Niemiec:** *Cyber Security Strategy for Germany*.	**Cybercrime**	**Cyberprzestępstwo**
17.	**2011**	**Rządowy program Francji:** *Défense et sécurité des systèmes d'information Stratégie de la France*.	**Cybercriminali-té**	**Cyberprzestępstwo**
18.	**2011**	**Rządowy program Holandii:** *The National Cyber Security Strategy* [...].	**Cybercrime**	**Cyberprzestępstwo**

19.	2013	**Rządowa polityka Polski:** Polityka Ochrony Cyberprzestrzeni RP.	**Cyberprzestęp-stwo**	**Cybercrime (oficjalna wer. ang.)**

Przygotowane zestawienie uwidacznia stopniowy rozwój stosowanej terminologii w zakresie nazywania fenomenu przestępczości cybernetycznej. Chronologicznie pierwsze określenie - „nadużycie komputerowe", stosowane było głównie w latach siedemdziesiątych oraz osiemdziesiątych ubiegłego stulecia. W latach kolejnych, sformułowanie to ustąpiło miejsca nowym wyrażeniom, między innymi pojęciom „przestępstwa związanego z komputerem" oraz „przestępstwa komputerowego", niekiedy stosowanym wręcz synonimicznie.

Na gruncie poszczególnych dokumentów czasami występowały także nowe, oryginalne określenia, jak np. „przestępstwo powiązane z technologią informacyjną", czy też znane z ustawodawstwa brytyjskiego „bezprawne użycie komputera", choć wyrażenia te nie rozszerzyły swojego zakresu obowiązywania. Ostatecznie, wraz z początkiem nowego milenium popularność zdobyło pojęcie „cyberprzestępstwa", które wprowadzone zostało do obrotu międzynarodowego za sprawą Konwencji Budapesztańskiej oraz następnie rozpropagowane przez administrację rządową USA. Zdecydowana większość aktualnych dokumentów - w tym brytyjskich, wykorzystuje właśnie to ostatnie określenie, nawiązując jednocześnie do koniecznych regulacji cyfrowej domeny cyberprzestrzeni. Samo sformułowanie „cyberprzestępstwo" najczęściej pisane jest jako pojedynczy wyraz, choć w doktrynie angielskiej przyjęło się zapisywać je w postaci rozłącznej, jako „cyber przestępstwo". Z uwagi na swoją aktualność, w dalszych częściach pracy posługiwano się właśnie pojęciem „cyberprzestępstwa", które poprzez zastosowanie wspólnego przedrostka koresponduje także z wykorzystywanym pojęciem „cyberprzestrzeni".

Przechodząc do podsumowania najistotniejszych elementów definicyjnych analizowanych w rozdziale pojęć opisujących przestępczość w cyberprzestrzeni, wskazać należy następujące cechy charakteryzujące analizowany fenomen:

– systemy teleinformatyczne oraz sieci służyć mogą zarówno do popełniania przestępstw tradycyjnych, jak oszustwo, czy zniewaga, jak również przestępstw, które pojawiły się dopiero wraz z nadejściem cyberprzestrzeni, *vide* włamywanie się do zasobów komputerów, czy przechwytywanie transmisji danych,

- przestępstwa popełniane w cyberprzestrzeni nie ograniczają się metodologicznie wyłącznie do dokonywania określonych czynności technicznych, mających na celu, np. przełamanie zastosowanych na serwerze zabezpieczeń, ale mogą polegać także na wykorzystywaniu metod socjotechnicznych, mających na celu wprowadzenie użytkownika w błąd i np. podanie swojego hasła do skrzynki pocztowej w przekonaniu, że aktywuje nowe, darmowe usługi,
- regulacja karna penalizująca poszczególne cyberprzestępstwa nie musi odnosić określonego czynu wprost do systemów teleinformatycznych. Zakwalifikowanie popełnionego czynu do cyberprzestępczości winno odbywać się w oparciu o kryteria materialne, odwołujące się do sposobu oraz miejsca popełnienia danego czynu, nie zaś formalne,
- systemy oraz sieci mogą występować w zjawiskach przestępnych w dwór rolach: jako narzędzie oraz jako cel. W przypadku przestępstw zamykających się w całości w cyberprzestrzeni role te występują równolegle,
- pojawienie się obszaru cyberprzestrzeni wykreowało nowe środowisko dla działań bezprawnych, powodując nie tylko, że *miejscem* popełniania nowoczesnych przestępstw jest *de facto* logiczny obszar domeny cyfrowej, ale także zmieniając sposób rozumienia dobra prawnie chronionego stanowiącego przedmiot zamachu. Cyberprzestępczość nierzadko kierowana jest przeciwko samemu bezpieczeństwu systemów teleinformatycznych oraz przetwarzanych na nich danych w postaci elektronicznej. W zależności od rodzaju danych możliwe jest też dalsze kwalifikowanie czynu, np. jako kradzież w przypadku przesuwania aktywów finansowych pomiędzy kontami w atakowanej usłudze bankowości elektronicznej,
- przestępczość cyberprzestrzeni może być popełniana zarówno poprzez bezpośrednie działanie sprawcy, jak również zautomatyzowane działania odpowiednio przygotowanego systemu lub oprogramowania. Dla przykładu, wirus komputerowy może wykraść dane oraz wysyłać je do swojego autora nawet po kilku latach od umieszczenia go w sieci,
- z uwagi na sposób popełniania cyberprzestępstw, ściganie ich sprawców wymaga podejmowania wielu czynności technicznych pozwalających na odnajdywanie elektronicznych dowodów przestępstwa. Pozyskiwanie takich dowodów wymaga przede wszystkim zabezpieczania fizycznych nośników danych oraz tzw. *logów* wskazujących historię ruchu sieciowego,

– pośród najczęściej wymienianych *cyberprzestępstw* znaleźć można bezprawny dostęp do danych lub systemu (dostęp do systemu nie musi wiązać się z dostępem do chronionych danych, może zaś ograniczać się jedynie do części konfiguracyjnej), uszkadzanie danych, zakłócanie poprawnego funkcjonowania systemu, udostępnianie narzędzi służących do popełniania przestępstw w cyberprzestrzeni (np. tzw. *exploit'ów* będących gotowymi programami przygotowanymi do wykorzystania określonej podatności systemu), propagowanie w sieciach treści zabronionych, czy nielegalne powielanie materiałów chronionych prawami autorskimi lub naruszanie takich praw w inny sposób. Dodać należy, że każde z cyberprzestępstw może być popełnione na wiele sposobów technicznych - nazywanych także atakami, odnoszących się do *modus operandi* sprawcy.

W ocenie autora, pełne ujęcie zjawiska cyberprzestępczości wymaga łącznego obejmowania wszystkich wskazanych powyżej cech, *de facto* wynikających (czy wręcz wywodzących się) z definicji różnych pojęć wymienionych na gruncie rozdziału.

Rozdział III
Technologia cyberprzestrzeni

§1. Podstawy budowy oraz funkcjonowania komputerów

Jak zostało zauważone w poprzednim rozdziale, jednym z podstawowych elementów cyberprzestrzeni jest podbudowująca ją technologia, uwzględniana we wszystkich wskazywanych wcześniej definicjach. Składają się na nią zarówno elementy infrastrukturalne rozległych sieci telekomunikacyjnych (np. centrale, czy linie), urządzenia końcowe zlokalizowane w biurach i domach poszczególnych użytkowników, jak i warstwa programowa obsługująca proces szeroko rozumianego przetwarzania danych w postaci elektronicznej. Składniki te tworzą wspólnie zbiór powiązanych ze sobą fizycznie oraz funkcjonalnie mikro- i makroelementów. W efekcie subtelnej, cyfrowej symbiozy łączącej cyberprzestrzeń z napędzającą ją technologią, kształt oraz sposób funkcjonowania cyberprzestrzeni pozostają w ogromnej mierze uzależnione od możliwości, ale także ograniczeń, charakteryzujących zastosowane do jej budowy rozwiązania sprzętowe oraz programowe.

Pomimo prawniczego charakteru pracy, szerokie ujęcie specyfiki przestępczości popełnianej w obszarze cyberprzestrzeni oraz środków procesowych podejmowanych w celu ich ścigania, wymaga tym samym także bliższego przyjrzenia się samej warstwie technologicznej cyfrowej domeny. Na uwzględnienie zasługują przy tym nie tylko podstawowe informacje o działaniu komputerów oraz przetwarzaniu danych, włączając w to ich przechowywanie, ale także budowa oraz funkcjonowanie nowoczesnych sieci teleinformatycznych, ze szczególnym uwzględnieniem Internetu. Będąc bowiem siecią o zasięgu globalnym, to właśnie Internet stanowi dziś jeden z najważniejszych ilościowo składników cyberprzestrzeni, znajdując swoje odzwierciedlenie w każdej jej definicji, niezależnie od tego, czy wymieniany jest tam wprost z nazwy, czy wprowadzany w postaci opisowej. Charakterystyka wymienionych technologii cyberprzestrzeni, przedstawiająca informatyczne podstawy jej funkcjonowania, pozwoli zatem nie tylko na dalsze rozwinięcie jednego z podstawowych elementów definicyjnych tego obszaru, ale przede wszystkim – na osadzenie specyfiki zwalczania cyberprzestępczości w ramach technologicznych, niezbędnych dla pełnego (także praktycznego) zrozumienia tak samego zjawiska

cyberprzestępczości, jak i metod wykrywania oraz zwalczania jego przejawów. Tak samo bowiem, jak terenowa praca dochodzeniowo-śledcza wymaga znajomości podstaw kryminalistyki z zakresu patologii, daktyloskopii, czy traseologii, tak też zwalczanie zagrożeń występujących w cyberprzestrzeni wymaga bliższego poznania zasad działania tego osobliwego środowiska, w którym *nie-fizyczne* czynności pozostawiają równie *nie-fizyczne* ślady, których dostrzeżenie oraz zrozumienie nie jest możliwe bez wiedzy na temat, jak działają komputery oraz sieci[1].

Niniejszy rozdział został podzielony na trzy części, poświęcone odpowiednio podstawom budowy oraz działania komputerów, budowie nowoczesnych sieci teleinformatycznych – głównie w kontekście budowy Internetu oraz przeglądowi zagadnień związanych z posługiwaniem się elektronicznymi nośnikami danych. Należy zauważyć, że podział ten mając charakter czysto porządkowy, został zaproponowany jedynie by zapewnić czytelny sposób wprowadzenia poruszanej materii. W szczególności zatem, nie należy odbierać go jako próby wprowadzenia podziału cyberprzestrzeni na mniejsze części składowe, bowiem w praktyce Internet nie działa przecież bez budujących go komputerów oraz serwerów, zaś te składują przetwarzane dane na wbudowanych, czy podłączonych nośnikach pamięci, jak choćby dyskach twardych. Poprawna współpraca wszystkich komponentów technicznych wymaga natomiast stosowania kompatybilnych rozwiązań programowych opierających się na wspólnych protokołach komunikacyjnych.

Szeroka dostępność nowoczesnych technologii, wiążąca się w ogromnej mierze z obniżeniem kosztów produkcji układów scalonych, spowodowała, że w dzisiejszych czasach posiadanie w domu prywatnego komputera, dodatkowo podłączonego do Internetu, stało się czymś zupełnie naturalnym. Szacunkowo w roku 2005 na świecie wykorzystywanych było ponad dziewięćset milionów komputerów[2], podczas gdy na rok 2014 liczba ta była kalkulowana już na poziomie dwóch miliardów. Obecnie, średnia roczna liczba komputerów osobistych wprowadzanych do sprzedaży w danym roku kalendarzowym osiąga wartości oscylujące na poziomie 300 milionów sztuk[3]. Z pewnością dane te musiały być niewyobrażalne dla autora słów pochodzących z 1949 r., który prognozował, że: „O ile

1 M. Cross, D. Littlejohn Shinder, *Scene of the Cybercrime*, Syngress 2008, s. 122.

2 Dane przedstawione w dniu 22 maja 2006 r. przez amerykański serwis *Computer Industry Almanac*, dostępne na stronie internetowej pod adresem: http://www.c-i-a.com/pr0506.htm. Jak wynika ze szczegółowego zestawienia jedna czwarta tej liczby przypadała na same USA.

3 Na podstawie danych firmy analitycznej Gartner, powoływanych na stronie internetowej pod adresem: http://www.marketwatch.com/story/gartner-lowers-2011-forecast-for-pc-shipments-2011-09-08 oraz dane portalu Statista, dostępne na stronie internetowej pod adresem: http://www.statista.com/statistics/263393/global-pc-shipments-sine-1st-quarter-2009-by-vendor.

ENIAC [jeden z pierwszych komputerów][4] ma 18.000 lamp próżniowych i waży 30 ton, to jest możliwe, że komputer w przyszłości będzie miał tylko 1.000 lamp próżniowych i ważył tylko 1,5 tony”[5]. Jako ciekawostkę warto dodać, że wydajność wspomnianego *super-komputera* ENIAC oscylowała na poziomie 500 *flopsów*[6], podczas gdy moc obliczeniowa współczesnych serwerów[7] znacznie przekracza wartość 500 *tera-flopsów* (10^{12}) – czyniąc je w porównaniu do swojego protoplasty 1.000.000.000.000 – bilion razy mocniejszymi. Ta ogromna moc współczesnych komputerów, nieustannie rozwijająca się w postępie wykładniczym, pozostaje także w ścisłej korelacji z codziennie rosnącą ilością przetwarzanych przez komputery danych. Ich przekazywanie oraz składowanie wymaga w efekcie stosowania równie wydajnych nośników, które zapewniają nie tylko niezbędną pojemność, ale także szybkość odczytu i zapisu danych. Z punktu widzenia zwalczania nowoczesnych form przestępczości, ten ogrom danych powoduje, że wykrycie, a czasem nawet samo wyszukanie informacji ważnej z punktu widzenia procesu karnego, nierzadko przybiera formę przysłowiowego szukania igły w stogu siana. Jej znalezienie bez zaprzęgnięcia specjalistycznych narzędzi tzw. informatyki śledczej, pozwalających automatycznie filtrować dane[8], czy prowadzić tzw. heurystykę, stanowiłoby nieosiągalne wyzwanie nawet dla najlepszych *cyber-dochodzeniowców*. Temat ten przeanalizowano nieco szerzej w punkcie trzecim niniejszego rozdziału.

Obok przytoczonej wyżej prognozy półtoratonowych komputerów, *przyszłość* zweryfikowała także absolutną błędność innych sceptycznych wobec komputeryzacji założeń stanowiących, że prywatny rynek komercyjny nigdy nie zainteresuje się komputerami, zaś nadmierny rozwój technologii cyfrowych podważy lub wręcz wyeliminuje rozwój intelektualnej działalności człowieka. Niezwykle celne oraz w istocie wciąż nieodbiegające istotnie od współczesnej rzeczywistości, okazało się natomiast sformułowane w 1965 r. przez Gordona Moore’a (współzałożyciela firmy Intel będącej jednym z dwóch głównych, obok

[4] Jeden z pierwszych komputerów, skonstruowany w 1945 r., ostatecznie uruchomiony do użytku dwa lata później. Jego podzespoły zainstalowane były w 42 stalowych szafach, ustawionych w prostokącie o wymiarach 12 na 6 metrów.

[5] J. S. Zieliński, Społeczeństwo Informacyjne, praca zbiorowa pod red. J. Papińska-Kacperek, , Wydawnictwo Naukowe PWN, Warszawa 2008, s. 69. Informacja opublikowana oryginalnie w: *Popular Mechanics*, marzec 1949 r.

[6] Jednostka miary wydajności komputerów.

[7] Np. rozwiązania IBM, więcej na ten temat na stronie internetowej pod adresem: http://domino.research.ibm.com/comm/research_projects.nsf/pages/bluegene.index.html.

[8] Na szczególne rodzaje narzędzi analitycznych zdolnych agregować oraz przetwarzać dane różnego rodzaju oraz formatu uwagę zwracają E. Nawarecki, G. Dobrowolski, A. Byrski, M. Kisiel-Drochnicki w: *Agent-Based Integration of Data Acquired from Heterogenous Sources*, cyfrowa biblioteka IEEE, czy też G. Dobrowolski, E. Nawarecki, J. Dajda, A. Byrski, M. Kisiel-Drohinicki, *Scenario-Driven Systems for Open Source Intelligence, Multimedia Communications, Services and Security*, CCIS *vol.* 287, Springer 2012.

AMD, producentów procesorów komputerowych) tzw. prawo Moore'a[9], stanowiące, że średnio co dwa lata podwaja się liczba tranzystorów umieszczanych na układach scalonych. W rozwinięciu, zasada ta została przełożona przez Davida House'a na osiemnastomiesięczny cykl dwukrotnego wzrostu mocy obliczeniowej dostępnych na rynku technologii, wynikający z - obok zwiększającej się liczby stosowanych elementów półprzewodnikowych, także rosnącej wydajności samych tranzystorów. Być może zatem futurystyczne wizje cyberprzestrzeni oraz wirtualnej rzeczywistości przedstawiane w powieściach Williama Gibsona[10], nie są wcale tak nierzeczywiste i odległe, jak może dzisiaj się nam wydawać?

Współczesne komputery - zarówno domowe, jak i dedykowane stacje robocze, zbudowane są z szeregu funkcjonalnie połączonych komponentów. Ich ścisła współpraca wymuszona jest określonym przeznaczeniem każdego z nich do realizacji wybranych kategorii zadań, powodując niesamodzielność poszczególnych części. Do najważniejszych podzespołów komputerowych zalicza się płytę główną z wbudowanymi interfejsami wejścia/wyjścia, gniazdem lub gniazdami procesora oraz portami na pozostałe komponenty – stanowiącą rodzaj podstawy komputera zespalającej wszystkie części; procesor (CPU – *Central Processing Unit*) nazywany także „sercem komputera"; pamięć operacyjną (*Random Access Memory*); nośniki magazynujące dane oraz napędy (w tym głównie dyski HDD, SSD, napędy DVD, Blu-ray); wreszcie układy: graficzny i dźwiękowy. W nowoczesnych płytach głównych zarówno układy graficzne, dźwiękowe, jak i karty sieciowe, w tym zapewniające łączność bezprzewodową, nierzadko stanowią część wyposażenia samej płyty. Oprócz wcześniej wymienionych komponentów należy zaznaczyć także istotną rolę urządzeń chłodzących (aktywnych - wentylatorów oraz pasywnych - radiatorów), bez których nowoczesne komputery nie mogłyby funkcjonować. Przy rozmiarze wewnętrznych elementów procesora na poziomie 32 nanometrów (nm = 0,0000001 cm) ich utkanie staje się niezwykle gęste, zaś optymalna temperatura pracy procesora, przy średnim obciążeniu, nie powinna przekraczać 50 stopni Celsjusza. Bez chłodzenia (oraz wyłącznika awaryjnego) mocno obciążony procesor momentalnie wytwarza temperaturę dochodzącą nawet do 300 (!) stopni Celsjusza, spalając się w przeciągu kilku sekund.

Opisana budowa modułowa, która towarzyszyła nowoczesnym komputerom opartym na układach scalonych od początków ich historii, a zatem połowy lat siedemdziesiątych XX

---

9 FLOPS (*Floating Point Operations Per Second*) – miara mocy obliczeniowej komputerów wyrażająca liczbę operacji zmiennoprzecinkowych na sekundę. Więcej na ten temat np. na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/FLOPS.

10 Np. W. Gibson, Neuromancer, Ace Books, Nowy York 1984.

w.[11], pozwala nie tylko dopasowywać konfiguracje komputerów do konkretnych potrzeb, ale także w prosty sposób wymieniać uszkodzone podzespoły oraz modernizować lub rozszerzać funkcjonalność całego zestawu. Należy mieć jednak w tym miejscu na uwadze, że kompatybilność poszczególnych technologii jest w pewnym zakresie ograniczona, co obok zastosowanych rozwiązań sprzętowych, pozostaje uzależnione także od polityki oraz rywalizacji ich producentów.

Wszystkie wymienione powyżej komponenty mają za zadanie realizować cztery podstawowe funkcje komputera, pozwalające opisać każdą możliwą do wykonania operację: przyjmować dane (*input*), przetwarzać je (*process*), wydawać efekt (*output*) oraz ewentualnie przechowywać (*storage*) – co nazywane jest łącznie, zbudowanym od pierwszych liter oryginalnych określeń, cyklem IPOS[12]. Przekładając cykl IPOS na poszczególne elementy komputera - w prostym zarysie, komputer najpierw otrzymuje dane wejściowe wprowadzane np. z nośników, łączy lub przy użyciu klawiatury (funkcje płyty głównej oraz urządzeń peryferyjnych); w kolejnym kroku przetwarza je w ściśle określony, zadany sposób, za co odpowiedzialny jest głównie, choć nie wyłącznie, procesor; wygenerowane efekty obliczeń przekazywane są z procesora do innych podzespołów, między innymi ulotnej pamięci operacyjnej RAM, skąd mogą być ponownie pobrane do wykonania dalszych operacji; oraz ostatecznie, wyniki obliczeń zapisywane są na nośnikach zapewniających trwałe – to znaczy nieprzerywane wyłączeniem komputera z prądu, magazynowanie danych. Należy podkreślić, że ostatni element cyklu – przechowywanie (*storage*) nie jest elementem niezbędnym i w zależności od funkcjonalności wykorzystywanego programu oraz woli użytkownika może nie występować, stąd też cykl IPOS nazywany jest często cyklem IPO+S. Innymi słowy, nie wszystkie operacje wykonywane na komputerze poddawane są trwałemu zapisowi, co z punktu widzenia zwalczania cyberprzestępczości, ma zasadnicze znaczenie dla zapewnienia poprawnego przebiegu procesu wykrywania oraz zabezpieczania dowodów.

Przyglądając się zachodzącym w komputerze procesom nieco bliżej, na najniższym (fizycznym) poziomie komputery, będące urządzeniami elektronicznymi, w dalszym ciągu – tak jak na początku swojej historii, *nie rozumieją* pojęć, jak „dane", przetwarzanie", „perspektywa", czy „grawitacja", ani choćby najprostszych poleceń typu „pomnóż" bądź „przenieś". Operują one zmiennymi stanami napięcia elektrycznego pojawiającego się w poszczególnych tranzystorach. Prąd płynący w obwodzie umownie interpretowany jest jako

[11] J. S. Zieliński, Społeczeństwo Informacyjne, op. cit., s. 54.

[12] Więcej na stronach internetowych pod adresami: http://www.ehow.com/about_4608753_what-four-basic-functions-computer.html, czy http://en.wikipedia.org/wiki/IPO_Model.

wartość „1”, zaś brak napięcia lub jego spadek poniżej określonego poziomu to „0”. Wyłącznie te dwie wartości, będące jednocześnie najmniejszymi jednostkami informacji - nazywanymi bitami[13], składają się na specyficzny język maszyn określany mianem języka binarnego[14], który stanowi podstawę funkcjonowania oraz komunikacji nowoczesnych komputerów. Dzięki kolejnym poziomom szeroko rozumianej warstwy programowej (od najniższej - obsługującej funkcjonowanie samego sprzętu; dalej systemowej; na końcu aplikacyjnej), dwuliterowy język binarny wykorzystywany jest do budowy oraz wykonywania coraz to bardziej złożonych wyrażeń. Z zastosowanej, odpowiedniej interpretacji ciągów zer i jedynek, budowane są najpierw litery oraz cyfry, z nich składane słowa i liczby, dalej funkcje, wreszcie całe polecenia itd. Dla prostego przykładu, zapisany słownie wyraz „witaj” (w postaci tzw. kodu ASCII), przekłada się na postać binarną:

01110111 01101001 01110100 01100001 01101010[15].

Co nietrudno zaobserwować na powyższym przykładzie, na potrzeby optymalizacji pracy, drobne *bity* składane są ósemkami w nieco większe *bajty* (z angielskiego *byte*[16]), będące najmniejszymi adresowalnymi (w uproszczeniu - identyfikowalnymi) jednostkami informacji pamięci komputerowej[17]. Jak łatwo policzyć, ośmiobitowy bajt posiada 256 (2^8) unikatowych wartości (kombinacji *bitów*).

Wracając jednak do rozważań dotyczących funkcjonowania kolejnych warstw oprogramowania - na podkreślenie zasługuje ostatecznie fakt, że programy wyższego poziomu wykorzystują funkcjonalności zaimplementowane na poziomach niższych, dzięki czemu raz zdefiniowane pojęcia oraz funkcje nie muszą być powtarzane (np. instalowane aplikacje bazują na możliwościach systemów operacyjnych, tworzących rodzaj środowiska pracy). Hierarchia ta ułatwia tworzenie programów najwyższego poziomu. Ujmując syntetycznie powyższe rozważania, zadaniem oprogramowania jest zatem swoiste pośredniczenie pomiędzy użytkownikiem, a sprzętowymi komponentami komputerów, wyrażające się w dwukierunkowym tłumaczeniu języków maszynowego oraz ludzi umożliwiające przyjmowanie oraz realizację poleceń przez komputery. W żargonie informatycznym, warstwę programową określa się także pochodzącym z języka angielskiego

[13] Więcej na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Bit.
[14] Więcej na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Binary_code.
[15] Kod binarny wygenerowany przy użyciu konwertera na stronie internetowej pod adresem: http://www.convertbinary.com/.
[16] Wyrażenie nawiązuje do angielskiego słowa *bite* – w znaczeniu „kęs”, co odnosi się do funkcji bajtów, tworzących najmniejsze adresowalne jednostki.
[17] Więcej na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Byte.

pojęciem *software*, pozostającym w opozycji do wyrażenia *hardware*[18], które stosowane jest dla określenia fizycznej warstwy sprzętowej.

Ponieważ samo budowanie programów w surowym języku binarnym, wymagającym dokonywania wielu mozolnych przeliczeń w celu przekonwertowania go na czytelne wyrażenia, pozostaje uciążliwe nawet dla doświadczonych informatyków, niezwykle długie ciągi zer i jedynek, składające się na wykonywany przez procesor kod maszynowy[19], budowane są przy zastosowaniu tzw. języków programowania wyższego rzędu[20], umożliwiających słowne zapisywanie poleceń, np.

if (switch == 1) light = 1; else light = 0; [21]

- powyższa formuła oznacza, że o ile wartość pobieranej zmiennej „*switch*" równa się „1", to wartość zmiennej „*light*" również przyjmuje „1", w innym zaś przypadku („*if else*"), wartość zmiennej „*light*" to „0". Tak zapisany kod źródłowy, w przytoczonym przykładzie sporządzony w popularnym języku programowania C++, poddawany jest następnie procesowi kompilacji lub asemblacji (w zależności od poziomu, do którego należy stosowany język programowania) w ramach którego sporządzane jest jego „tłumaczenie" na wykonywalny przez komputer kod maszynowy. Technicznie możliwy, choć wymagający wysokich umiejętności i zasadniczo niedopuszczalny w przypadku legalnego oprogramowania (z uwagi na ochronę praw autorskich) jest także proces odwrotny, nazywany dekompilacją, pozwalający odtwarzać fragmenty kodu źródłowego na podstawie wcześniej skompilowanego kodu maszynowego. W kontekście zwalczania przestępczości, dokonanie dekompilacji może być istotne np. dla przeprowadzenia pełnej analizy funkcjonalności programu służącego działalności przestępnej, choć samo podpatrzenie, krok po kroku, kolejnych operacji wykonywanych przez program możliwe jest także w procesie tzw. *debugowania*[22] polegającego na uruchomieniu programu w swojego rodzaju środowisku testowym. Należy zaznaczyć, że analogiczną budowę kodu źródłowego posiadają także strony internetowe, które również budowane są z zastosowaniem odpowiednio dobranych języków oprogramowania, m. in. HTML[23], czy PHP[24], posiadających swój własny zasób komend oraz

---

[18] Więcej na stronie internetowej pod adresem: http://www.ehow.com/how-does_4963751_how-pc-works.html.
[19] Więcej na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Machine_code.
[20] Np. C, C++, Pascal, Fortran, Cobol, czy BASIC , ale także wiele innych. Należy zauważyć, że poszczególne języki programowania często tworzone są pod kątem wykorzystywania ich do budowy określonych rozwiązań, np. język PHP służy do kodowania operacji wykonywanych przez serwery na stronach internetowych.
[21] Przykład zaczerpnięty ze strony internetowej pod adresem: http://www.tweak3d.net/articles/binary/.
[22] Więcej na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Debugging.
[23] *Hyper Text Markup Language* (hipertekstowy język znaczników). Więcej o HTML na stronach internetowych pod adresami: http://www.w3schools.com/html/, oraz http://pl.wikipedia.org/wiki/HTML.
[24] *PHP: Hypertext Preprocessor*, oryginalnie nazwa PHP pochodziła od skrótu *Personal Home Page*. Więcej o

specyficzną składnię.

Języki programowania wyższego rzędu pozwalają programować komputer do przetwarzania danych, wykonywania skomplikowanych funkcji matematycznych, czy obróbki grafiki, z zastosowaniem tzw. mnemonicznych (łatwych do zapamiętania) poleceń. Tworzone w ten sposób programy „ubierane są” na samym końcu w przyjazne dla użytkowników interfejsy, które stosując czytelną postać graficzną, w intuicyjny sposób prezentują oraz udostępniają rozliczne funkcje oferowane przez oprogramowanie. W efekcie, nawet najbardziej skomplikowane polecenia mogą być zadawane za pośrednictwem prostych ruchów oraz kliknięć przycisków myszki. Co warto zauważyć, także te proste działania użytkowników stanowią formę programowania komputerów.

Opierając się na tym, co zostało wskazane powyżej, oprogramowanie stanowi jeden z podstawowych elementów komputerów, równie niezbędny dla ich funkcjonowania, jak sam *hardware*. Bliższe poznanie funkcjonalności stosowanych najczęściej programów, w tym systemów operacyjnych, bazujące także na wiedzy dotyczącej działania samych komputerów, stanowi w konsekwencji jedną z podstawowych przesłanek poprawnego prowadzenia czynności śledczych oraz wykrywczych, podejmowanych w ramach postępowań dotyczących przestępczości komputerowej. Nieznajomość zasad działania oprogramowania, coraz częściej działającego w sposób w pełni zautomatyzowany poprzez formę tzw. agentów[25], może bowiem prowadzić nie tylko do nieujawniania istotnych dowodów, np. poprzez nieumiejętność dokonania oceny rzeczywistego zachowania danego programu (czy też strony internetowej) lub dotarcia do określonych zasobów, ale wręcz ich utratę, w drodze nawet najbardziej przyziemnych błędów, jak choćby poprzez nierozważne wyłączenie zabezpieczanego komputera bez uprzedniego sprawdzenia, czy znalezione w nim istotne dowodowo dane, chwilowo rezydujące jedynie w ulotnej pamięci RAM lub *cache*, zostały zachowane w sposób umożliwiający ich późniejsze odtworzenie[26]. Ilość dostępnych na rynku programów (oraz ich wersji), które pochodzą także od różnych producentów stosujących swoje własnościowe, często bardzo różne rozwiązania, z pewnością nie ułatwia pracy technikom – twierdzenie to w szczególności dotyczy wymagających szybkości oraz bezbłędności działań w terenie.

Przybliżając budowę oraz zasady działania komputerów, warto wskazać także na osobliwe fizyczne zjawisko tzw. elektromagnetycznej emisji ujawniającej (*compromising*

PHP na oficjalnej stronie internetowej języka programowania pod adresem: http://www.php.net/.

[25] Więcej na ten temat G. Dobrowolski, E. Nawarecki, Sytuacje kryzysowe w systemach agentowych, Automatyka 2005, tom 9, zeszyt 1-2, Kraków 2005.

[26] M. Cross, D. Littlejohn Shinder, op. cit., s. 127 – 128 oraz s. 150.

emmanation), w istocie towarzyszące funkcjonowaniu każdego urządzenia elektrycznego, czy elektronicznego. Każda operacja wykonywana przez procesor, dysk twardy, czy nawet związana z wyświetlaniem obrazu na komputerowym monitorze, wiąże się z generowaniem słabego pola elektromagnetycznego, wynikającego z przepływających w urządzeniach impulsów elektrycznych. Stosując odpowiednio przystosowane narzędzia, możliwe jest podsłuchiwanie tej emisji, pozwalające na zdalne, to znaczy bez żadnego kontaktu fizycznego, przechwytywanie np. aktualnego obrazu wyświetlanego na czyimś monitorze CRT lub LCD (ten konkretnie rodzaj ataku nazywany jest od nazwiska holenderskiego odkrywcy *Van Eck phreaking*[27]) lub podsłuchiwanie wpisywanych na klawiaturze znaków[28]. Działania takie mogą z jednej strony przybierać charakter przestępczy, ale z drugiej – używane w granicach prawa, służyć także na potrzeby wymiaru sprawiedliwości, zarówno na etapie czynności operacyjno-rozpoznawczych, jak i w ramach prowadzonych czynności procesowych.

§2. Podstawy budowy oraz funkcjonowania sieci komputerowych, ze szczególnym uwzględnieniem Internetu

Wykorzystywanie nowoczesnych sieci komputerowych stało się współcześnie nieodzowną częścią samego posługiwania się komputerami. Stopień integracji obydwu technologii spowodował, że wyrażenie „włączyć komputer" nabrało obecnie znaczenia omalże synonimicznego do połączenia się z siecią (lub sieciami), zaś funkcjonalność sieciowa stała się dziś jedną z podstawowych funkcjonalności komputera. Nowoczesne sieci komputerowe, nazywane w żargonie informatycznym po prostu „sieciami" (z ang. *net*), występują dziś zupełnie powszechnie - zarówno w dużych korporacjach, jak i małych firmach, wszelkich punktach usługowych, na uczelniach, w szpitalach, jednostkach administracji, w komisariatach policji, ale także w naszej *prywatnej* codzienności. Swoje praktyczne zastosowanie sieci komputerowe znalazły bowiem we wszystkich obszarach ludzkiej aktywności, usprawniając przepływ danych oraz informacji, umożliwiając zawieranie oraz realizowanie umów na odległość, ułatwiając prowadzenie rozległych rejestrów, czy wreszcie wspomagając procesy zarządzania pracą.

---

27 Więcej o samym ataku: W. van Eck, *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*, praca dostępna na stronie internetowej pod adresem: http://cryptome.org/emr.pdf. W sieci dostępne są także (np. na portalu You Tube) prezentacje praktycznego zastosowania ataku.

28 Zagadnienie przechwytywania emisji klawiatury zostało szeroko przeanalizowane w: M. Vuagnoux, S. Pasini, *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*, dostępnej na stronie internetowej pod adresem: http://www.usenix.org/event/sec09/tech/full_papers/sec09_attacks.pdf.

W najprostszym ujęciu, sieć komputerowa to zorganizowane połączenie komputerów, umożliwiające wzajemną wymianę oraz współdzielenie danych za pośrednictwem określonych kanałów komunikacji[29]. Do budowy najmniejszej sieci potrzebne są zatem dwa komputery wyposażone w urządzenia sieciowe (karty sieciowe), protokół sieciowy, będący rodzajem komputerowego języka obsługującego przekazywanie danych, oraz łącze – bądź przewodowe, bądź radiowe, stanowiące nośnik dla przepływających pakietów danych

W zależności od skali sieci oraz jej architekturalnego stosunku do innych sieci, wyróżnia się tzw. sieci lokalne (LAN[30]) – np. wewnętrzne sieci biurowe, czy sieci domowe budowane w przypadku dzielenia jednego łącza internetowego na wiele komputerów za pomocą routera; oraz tzw. sieci rozległe (WAN[31]) – których nadrzędnym przedstawicielem jest Internet, zwany także *siecią sieci*[32]. W zależności od przyjętego rozwiązania, nierzadko dyktowanego względami bezpieczeństwa, sieci LAN mogą być zarówno odseparowane od innych sieci LAN i WAN, jak i zintegrowane z nimi, umożliwiając przeskok pomiędzy sieciami (np. wyjście z sieci biurowej na Internet).

Powyższa definicja sieci, określająca na pierwszy rzut oka nieskomplikowaną funkcjonalność, skrywa pod sobą wysublimowaną logikę sieciową, bez której niemożliwe byłoby wykonanie choćby najprostszego wydruku przy zastosowaniu współdzielonej drukarki sieciowej. Bez wdrożenia określonej architektury, zasad rysowania topologii wszelkich elementów sieciowych, przyjęcia określonych metod adresacji oraz zaimplementowania odpowiednich protokołów wymiany danych, wysyłanie oraz odbieranie pakietów danych nie byłoby w ogóle możliwe. Dla obrazowego przedstawienia kwestii, zastosować tu można analogię do funkcjonowania tradycyjnej poczty, w której każdy list musi spełniać pewne wymagania oraz posiadać określone cechy, zaś cały system pocztowy charakteryzować się zdolnością do ich zrozumienia oraz wykorzystania, tak by przesyłka dotarła od nadawcy do adresata.

Do schematycznego opisu budowy oraz działania sieci komputerowych stosuje się tzw. model OSI[33], przedstawiający strukturę sieci w postaci siedmiu współpracujących ze sobą warstw. Model OSI – w tłumaczeniu na język polski: model łączenia systemów

---

[29] Definicja zbudowana na podstawie materiałów ze stron internetowych pod adresami: http://www.ehow.com/facts_5478976_definition-computer-networking.html oraz http://en.wikipedia.org/wiki/Computer_network.

[30] Skrót pochodzi od anglojęzycznych wyrazów: *Local Area Network*.

[31] Skrót pochodzi od anglojęzycznych wyrazów: *Wide Area Network*.

[32] Tak np. na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Internet.

[33] *Open System Interconnection*. Skrót „OSI” wymawiany jest po polsku bez przekształcania zbitki liter „SI” na głoskę „ś”.

otwartych[34], został stworzony w połowie lat osiemdziesiątych przez Międzynarodową Organizację Normalizacyjną (ISO) oraz następnie zaktualizowany dziesięć lat później[35], w celu ustandaryzowania rozwiązań sieciowych dostarczanych przez różnych producentów. W połowie lat dziewięćdziesiątych XX w. model OSI został także przyjęty do systemu polskich norm.

Wedle założeń modelu OSI, sieć zbudowana jest z siedmiu, ułożonych hierarchicznie warstw: warstwy fizycznej, warstwy łącza danych, warstwy sieciowej, warstwy transportowej (tzw. warstwy niższe lub dolne) oraz warstwy sesji, warstwy prezentacji i warstwy aplikacji (tzw. warstwy wyższe lub górne)[36]. Warstwy te pozwalają opisać pełną drogę, jaką przebywają dane w ramach przekazywania ich pomiędzy komputerami, która w skrócie odbywa się od aplikacji jednego komputera, funkcjonującej w najwyższej warstwie sieci, w dół, aż do warstwy fizycznej służącej do przesłania budowanych przez ciągi zer i jedynek strumieni binarnych, by następnie przejść przez warstwy w odwrotnym kierunku – i dotrzeć do aplikacji komputera docelowego. Tym samym, komunikacja pomiędzy aplikacjami nie odbywa się bezpośrednio pomiędzy nimi, zaś jest dokonywana za pośrednictwem zdefiniowanych w modelu OSI warstw.

W miarę przekazywania danych pomiędzy warstwami sieci, dokonywana jest zmiana ich formatu, nazywana enkapsulacją[37]. Jednocześnie, dane dzielone są także na coraz mniejsze porcje, co wynika z przyjętych rozwiązań technicznych. Przetwarzany w warstwie transportu pakiet[38], składający się z danych właściwych (zawierających treść przekazu) oraz nagłówka segmentu, w kolejnym kroku, w warstwie sieciowej uzupełniany jest nagłówkiem sieciowym zawierającym logiczne adresy komputerów nadawcy oraz odbiorcy, pozwalające na wyznaczenie trasy pomiędzy zakończeniami sieci. Odczytanie nagłówków sieci pozwala zatem ustalić dane lokalizujące punkty, pomiędzy którymi doszło do wymiany danych. W warstwie łącza danych pakiet otrzymuje nagłówek ramki, określający sposób wymiany

---

[34] Więcej na stronach internetowych pod adresami: http://support.microsoft.com/kb/103884 oraz http://pl.wikipedia.org/wiki/Model_OSI.

[35] Model OSI zawarty jest w normie ISO 7498-1:1994, dostępnej na stronie internetowej pod adresem: http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip.

[36] Oryginalne, anglojęzyczne nazwy warstw to odpowiednio: *Physical layer, Data link layer, Network layer, Transport layer, Session layer, Presentation layer* oraz *Application layer*. Jako ciekawostkę, można wskazać popularną wśród informatyków technikę mnemoniczną służącą do zapamiętania wymienionych nazw w odpowiedniej kolejności: *Please do not throw sausage pizza away.* Pierwsze litery słów przytoczonego zdania są jednocześnie pierwszymi literami nazw kolejnych warstw. Ten oraz inne przykłady dostępne są na stronie internetowej pod adresem: http://www.tcpipguide.com/ free/t_OSIReferenceModelLayer Mnemonics.htm.

[37] Funkcja polegająca na zamykaniu (ukrywaniu) treści w kolejnych pakietach posiadających nowe oznaczenia. Więcej na temat enkapsulacji na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Encapsulation_(networking).

[38] W skrócie PDU – *Protocol Data Unit*.

danych oraz ostatecznie trafia do warstwy fizycznej, w której zamieniany jest w postać binarną oraz przesyłany dalej po łączach. Wędrując ku odbiorcy, pakiety danych przechodzą następnie w systemie docelowym pomiędzy kolejnymi warstwami modelu OSI odwrotnie – w górę, zgodnie z informacjami zawartymi w nadanych im wcześniej nagłówkach. Powykorzystaniu, nagłówki są zdejmowane, tak by dane docierały do aplikacji komputera odbiorcy w postaci oryginalnej. Za weryfikację bezbłędności transferu danych odpowiedzialne są warstwy dolne.

Do opisu budowy oraz funkcjonowania Internetu stosuje się także zamiennie model TCP/IP, stanowiący swoistą implementację modelu OSI. O ile model OSI jest modelem referencyjnym, nieodwołującym się do żadnych konkretnych protokołów wymiany danych, o tyle model TCP/IP opiera się na już na konkretnych rozwiązaniach, między innymi tytułowych protokołach TCP oraz IP – których pełne nazwy to odpowiednio *Transmission Control Protocol* oraz *Internet Protocol*. Model TCP/IP w postaci w pełni sformalizowanej został przyjęty w 1989 r. w normie RFC 1122[39] wydanej przez otwartą, międzynarodową organizację standaryzacyjną *Internet Engineering Task Force*[40] (stanowiącą forum dla w wypracowywania głównych zasad działania globalnej sieci), choć jego podstawy zostały stworzone jeszcze w latach siedemdziesiątych pod auspicjami amerykańskiej agendy rządowej DARPA[41], zajmującej się rozwojem technologii militarnych. W swoich korzeniach, Internet projektowany był jako rozproszona, odporna na ataki sieć wojskowa, pozbawiona centralnego punktu zarządzającego oraz posiadająca zdolność do automatycznego wyszukiwania możliwych dróg połączeń, na wypadek fizycznego zerwania niektórych łączy.

Analogicznie, jak w przypadku modelu OSI, także model TCP/IP zbudowany jest w oparciu o szereg logicznie wydzielonych warstw, których hierarchiczna budowa oraz wzajemne relacje pozwalają opisać zachodzące w sieci procesy. Inaczej niż w przypadku modelu OSI, model TCP/IP wyróżnia jednak nie siedem, lecz cztery następujące warstwy: warstwę dostępu do sieci, warstwę Internetu, warstwę transportową oraz warstwę aplikacji. Pomimo wyraźnej różnicy w kwestii sposobu podziału sieci na warstwy, oba modele są względem siebie odpowiadające. Z uwagi na oparcie struktur modeli ISO oraz TCP/IP na analogicznych rozwiązaniach sieciowych, warstwę aplikacji modelu TCP/IP funkcjonalnie przyrównać można do połączonych warstw: aplikacji, prezentacji oraz sesji - znanych

[39] Norma dostępna na stronie internetowej pod adresem: http://tools.ietf.org/html/rfc1122.

[40] W tłumaczeniu „Grupa zadaniowa inżynierii Internetu". Więcej o organizacji na jej oficjalnej stronie internetowej pod adresem: http://www.ietf.org/.

[41] *Defense Advanced Research Agency*. Oficjalna strona internetowa DARPA pod adresem: http://www.darpa.mil.

z modelu OSI; warstwę transportową modelu TCP/IP do jej imienniczki z modelu OSI; warstwę Internetu modelu TCP/IP do warstwy sieciowej modelu OSI; oraz wreszcie, występującą w modelu TCP/IP warstwę dostępu do sieci, do połączonych warstw łącza danych oraz fizycznej - z modelu OSI. Uproszczona, choć nie zubożona funkcjonalnie, budowa modelu TCP/IP ma na celu lepsze odzwierciedlenie etapów, w ramach których faktycznie wykonywane są procesy sieciowe.

Jak zostało zauważone wcześniej, model TCP/IP oparto na dwóch podstawowych protokołach komunikacji, tytułowych TCP oraz IP. Łącznie, stanowią one fundament dla całego ruchu sieciowego oraz bazę dla innych, nierzadko bardzo ważnych protokołów, uzupełniających funkcjonalność sieci, jak np. protokoły HTTP, czy DNS. Działające w różnych warstwach sieciowych protokoły komunikacyjne tworzą zbiory podstawowych zasad oraz instrukcji wymiany danych, odnosząc je, w zależności od protokołu, do danych w ogóle lub danych występujących w określonym formacie. Zadaniem protokołu TCP jest nawiązywanie oraz obsługiwanie połączenia pomiędzy dwoma fizycznymi zakończeniami sieci wykorzystywanymi do komunikacji. Protokół ten działa w warstwie transportowej. Pierwsza funkcja TCP – nawiązywanie połączenia, wykonywana jest w ramach procesu tzw. trójstopniowego uzgadniania[42], nazywanego w oryginale: *three-way handshake*[43]. W trakcie realizacji funkcji uzgadniania, host (stacja biorąca udział w komunikacji) inicjujący wymianę danych, wysyła cyfrowe zapytanie o synchronizację (pakiet SYN) do hosta, z którym ma nastąpić komunikacja. O ile ten wyraża zgodę na nawiązanie połączenia, co uwarunkowane jest jego konfiguracją, wysyła zwrotnie sygnał potwierdzający wraz z wnioskiem o wzajemną synchronizację (pakiet SYN-ACK). W odpowiedzi, host inicjujący połączenie odsyła ostatecznie informację potwierdzającą (pakiet ACK), co skutkuje ustanowieniem połączenia[44]. W protokole TCP host inicjujący nazywany jest także „klientem", zaś wywoływany „serwerem", przez co sam protokół określany jest także, jako działający w trybie klient-serwer.

W trakcie dalszej obsługi transmisji danych, protokół TCP odpowiedzialny jest za weryfikację poprawności przesyłania danych, co ma na celu uniknięcie dostarczania danych niekompletnych, uniemożliwiającego ich poprawny odczyt (w przypadku uszkodzenia struktury pliku, jego otwarcie może okazać się w ogóle niemożliwe). Do kontroli

---

[42] Tak np. internetowa strona wsparcia firmy Microsoft, dostępna pod adresem: http://support.microsoft.com/kb/287932/pl, czy internetowy słownik: http://www.diki.pl/slownik-angielskiego/?q=three-way+handshake.

[43] Więcej na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Transmission_Control_Protocol.

[44] Na podstawie: http://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml oraz http://support.microsoft.com/kb/172983.

poprawności transmisji stosowane są numery sekwencyjne pakietów, pozwalające na poprawne scalanie otrzymywanych danych oraz tzw. sumy kontrolne, które wyliczane są dla przekazywanych danych oraz przesyłane razem z nimi, a następnie porównywane z danymi otrzymanymi. O ile sumy kontrolne generowane przez obie strony komunikacji są jednakowe, transmisja weryfikowanych pakietów przebiegła bez zakłóceń. Pakiety zagubione przesyłane są ponownie. Ostatecznie, protokół TCP zakańcza połączenie stosując wzajemnie potwierdzaną przez hosty wymianę odpowiednich poleceń (pakiety FIN oraz ACK).

Drugi z wymienionych protokołów komunikacji, budujących podstawy opisującego Internet modelu TCP/IP – protokół IP, to w istocie serce globalnej sieci. Działający w warstwie Internetu (lub warstwie sieciowej w strukturze modelu OSI) protokół IP odpowiada za „geograficzne" wyznaczanie trasy przesyłanym przez sieć pakietom danych, nazywane także „trasowaniem". W uproszczeniu, protokół IP umożliwia hostowi, w sposób w pełni zautomatyzowany, określić dokładną ścieżkę prowadzącą poprzez łącza, węzły oraz inne elementy infrastrukturalne sieci, która umożliwi zestawienie logicznego połączenia pomiędzy stronami wymiany danych oraz dostarczenie pakietów do ich odbiorcy – czy to w ramach *surfowania* po stronach WWW, pobierania plików, czy wysyłania poczty elektronicznej.

Co istotne, wyznaczanie trasy jest procesem odbywającym się *ad hoc*, w toku natychmiastowej wymiany informacji pomiędzy kolejnymi urządzeniami budującymi łańcuszek połączeń, nie zaś w oparciu o wcześniej przygotowaną, globalną mapę[45]. Opisany sposób działania zezwala nie tylko na łączenie dowolnych punktów sieci pomimo braku bezpośrednich łączy, wydajne zarządzanie infrastrukturą sieci - maksymalizujące prędkość transmisji danych, ale także zapewnianie „objazdów" w przypadku wystąpienia jakichkolwiek awarii, poprzez możliwość wyszukiwania alternatywnych dróg połączeń (Internet przedstawia się często obrazowo jako pajęczynę, w której dwa dowolnie obrane punkty można połączyć na setki możliwych sposobów). Warto w tym miejscu przypomnieć, że w pierwotnym zamyśle Internet projektowany był na potrzeby wojskowe, jako sieć rozproszona, cechująca się zdolnością do zestawiania oraz utrzymywania połączeń nawet poprzez najodleglejsze sieciowe drogi w przypadku zniszczenia części pośredniczących węzłów. Kilkanaście lat później, w swoim cywilnym wcieleniu, protokół IP stał się jednym z filarów błyskawicznego rozrostu, a także sukcesu na wskroś komercyjnego Internetu.

[45] Do ustalania konkretnej trasy łączącej wykorzystywany komputer ze wskazanym hostem, w środowisku Windows służy komenda *"tracert_adres IP lub WWW badanej strony"* wpisywana w wierszu komend (aplikacja *cmd*).

Trasowanie ruchu sieciowego odbywa się przy zastosowaniu tzw. adresu IP[46], stanowiącego znormalizowany identyfikator zakończeń sieci Internet, do których podłączane są wszelkiego rodzaju sieciowe urządzenia – np. nasze komputery, czy serwery, na których wywieszane są strony WWW. Innymi słowy, to właśnie adres IP pozwala na identyfikowanie oraz fizyczne lokalizowanie punktów, pomiędzy którymi zachodzi wymiana danych. Co więcej, umożliwia on także ustalenie niezbędnej ścieżki, którą przekazywane pakiety danych będą musiały przebyć skacząc pomiędzy kolejnymi węzłami (również posiadającymi swoje adresy IP) aż dotrą do wskazanego im odbiorcy. W pewnym uproszczeniu, funkcję adresu IP można zatem porównać do funkcji numeru telefonu. Jednocześnie, tak jak numer telefonu nie zapewnia informacji o osobie, która podniesie słuchawkę, tak samo adres IP, wskazując wyłącznie na wykorzystywane zakończenie sieci, nie określa danych użytkownika, który faktycznie generuje ruch sieciowy (nie może być bezpośrednio utożsamiany ze sprawcą cyberprzestępstwa). Zupełnie inaczej niż w przypadku numerów telefonicznych, adres IP najczęściej przypisywany jest przez dostawcę usług sieciowych (tzw. ISP – *Internet Service Provider*) danemu zakończeniu sieci dynamicznie, wyłącznie na czas trwania sesji (w uproszczeniu połączenia), co oznacza, że jego aktualny dysponent może zmieniać się bardzo często, choć oczywiście w danym czasie jeden adres IP może być przypisany wyłącznie do jednego zakończenia sieci.

Z punktu widzenia ścigania przestępczości komputerowej opisane wyżej rozwiązanie powoduje konieczność weryfikowania, do którego zakończenia sieci przypisany był interesujący adres IP w ściśle określonym czasie wykorzystania go do popełnienia czynu przestępnego. Do przeprowadzania takich ustaleń wykorzystuje się tzw. logi (dzienniki) operatora, zawierające historię całego ruchu sieciowego, pełniące jednocześnie funkcję analogiczną do billingów w sieciach telefonicznych. Utrzymywane przez operatorów z mocy prawa[47] logi, pozwalają ustalić zorientowaną w czasie tablicę użytkowników poszczególnych adresów IP, stanowiąc także niezwykle cenne źródło dowodowe, mogące dostarczyć istotnych informacji na temat pochodzenia oraz przebiegu każdego rodzaju cyberprzestępstwa. Posługiwanie się tzw. stałymi adresami IP – polegające na czasowej (np. kilkuletniej) rezerwacji określonego adresu, stanowi dziś rzadkość, w szczególności zaś w przypadku

[46] Więcej o adresie IP na stronach internetowych: http://www.inetdaemon.com/tutorials/internet/ip/addresses/ip_address.shtml oraz http://en.wikipedia.org/wiki/IP_address.

[47] W polskim porządku prawnym odnośne regulacje zawarte są w przepisach ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) oraz wydanych na jej podstawie aktów wykonawczych.

użytkowników - osób fizycznych[48]. Co oczywiste, cechą cyberprzestępców jest nie tylko unikanie własnych stałych adresów, ale wykorzystywanie takich, które nie prowadzą do identyfikacji ich danych osobowych lub wręcz kierują podejrzenia na inne osoby – o czym szerzej w dalszych częściach niniejszego rozdziału, a także kolejnych rozdziałach poświęconych zagadnieniom cyberprzestępczości oraz problematyce procesowej.

Adres IP zapisywany jest najczęściej w postaci liczbowej (w systemie dziesiętnym), w podziale na cztery oddzielone kropkami oktety[49], czyli części zbudowane z ośmiu bitów, a zatem mogące przybierać wartości od 0 do 255 (w sumie 256 - 2^8), np.:

173.194.70.139

Tak określony format IP został przyjęty uniwersalnie dla całego obszaru Internetu, jako rozwiązanie jednoznacznie identyfikujące jedno konkretne zakończenie sieci, co zapewnia jego obsługę niezależnie od miejsc (w szczególności krajów), w których zlokalizowane są oba łączące się urządzenia sieciowe. Niezależnie zatem od tego skąd łączymy się z siecią, ani tego gdzie zlokalizowany jest nasz punkt docelowy, wpisanie jednego adresu IP spowoduje połączenie z tym samym hostem, np. tą samą stroną internetową. Jednocześnie przedstawiona budowa adresu IP narzuca skończoność dostępnej puli adresowej – adres IP, będący w sumie liczbą 32 bitową (4 x 8 bitów) może przybrać maksymalną wartość niewiele wyższą od czterech miliardów (dokładnie 2^{32} = 4,294,967,295). W praktyce, z uwagi na szczegółowe zasady adresacji oraz ogromne obciążenie Internetu, aktualnie pula adresowa została już w pełni rozdzielona pomiędzy kraje oraz zbliża się do wyczerpania, co stanowi jeden z powodów przejścia z obecnie wykorzystywanej technologii adresacji IPv4 na IPv6, gdzie liczba dostępnych adresów wzrośnie 10^{29} razy (adres IP będzie liczbą 128 bitową)[50].

Obok adresu IP istnieje także inny identyfikator służący do określania źródła ruchu sieciowego – nazywany MAC adresem (*Media Access Control*)[51]. Stanowiąc swojego rodzaju numer rejestracyjny wykorzystywanego urządzenia sieciowego (np. karty sieciowej zainstalowanej w komputerze) nie określa on jednak zakończenia sieci – tak, jak czyni to adres IP, lecz konkretny egzemplarz urządzenia zastosowanego do obsługi ruchu sieciowego,

---

48 Np. dwie najpopularniejsze w Polsce usługi dostępu do sieci - Neostrada (oferowana przez Telekomunikację Polską SA) oraz Chello (UPC) świadczone są wyłącznie w oparciu o adresy dynamiczne – a więc właśnie bez zastosowania adresów stałych, o czym można przeczytać na odnośnych stronach wsparcia technicznego: http://www.tp.pl/prt/pl/klienci_ind/obsluga_klienta/pomoc_tech/internet/neostrada_tp/par_neo/?_faq=685643&show_faq=true, oraz http://obsluga-klienta.upc.pl/app/answers/detail/a_id/49/session/L3NpZC9oRFRzc2FTaw%3D%3D/p/2.

49 Definicja dostępna na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Oktet_(informatyka).

50 Więcej na stronach internetowych pod adresami: http://pl.wikipedia.org/wiki/IPv4 oraz http://pl.wikipedia.org/wiki/IPv6.

51 Więcej na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/MAC_address.

pełniąc tym samym rolę zbliżoną do numeru IMEI[52], w który wyposażony jest każdy telefon komórkowy. Adres MAC zapisywany jest w postaci liczbowej (w systemie szesnastkowym – *heksadecymalnym*), przyjmując wartość 48 bitów (ilość potencjalnych unikatowych MAC adresów to 2^{48} = 281,474,976,710,656 - wartość znacznie przewyższająca liczbę potencjalnych adresów IP w standardzie IPv4), np.[53]:

1B-6B-D3-68-2A-8E

Zgodnie z przyjętym przez IEEE (*Institute of Electrical and Electronics Engineers*)[54] standardem, pierwsza połowa adresu MAC (24 bity) wskazuje producenta sprzętu, zaś jego druga część to unikatowy numer konkretnego egzemplarza urządzenia sieciowego. Pomimo identyfikacyjnej roli adresów MAC, które w zamierzeniu miały jednoznacznie określać urządzenia sieciowe, większość producentów modemów, routerów, czy kart sieciowych, wprowadza do swoich produktów możliwość swobodnej zmiany adresu MAC, która z jednej strony ułatwia konfigurację urządzeń sieciowych oraz pozwala unikać niechcianego szpiegowania ruchu w sieci (np. prowadzonego w celach marketingowych), lecz z drugiej – może być wykorzystywana przez cyberprzestępców chcących ukryć identyfikujące ich dane lub nawet podszyć się pod kogoś innego. Technicznie bowiem możliwe jest przechwycenie cudzego adresu MAC np. w trakcie podsłuchania transmisji bezprzewodowej (atak typu *man-in-the-middle*, opisany szerzej w dalszych częściach pracy) oraz sklonowanie go na własnym urządzeniu.

Wracając jednak do adresów IP - skoro zatem - zgodnie z tym, co zostało wskazane powyżej, adresy te są tak ważnym elementem funkcjonowania sieci, dlaczego zdecydowana większość internautów w ogóle się z nimi nie spotyka? Czy są zatem gdzieś ukryte? Otwierając strony internetowe, czy pobierając pliki, w polu adresowym nie wpisujemy przecież oddzielonych kropkami liczb, lecz zapisywane wyrazami (w postaci literowej) domeny np. www.google.com, które ewentualnie *łamiemy* dodatkowo dalszymi ścieżkami, doprecyzowującymi określony zasób - np. www.google.com/insights/search/#.

Dzieje się tak, ponieważ dla wygody internautów adresacja IP została rozwinięta o usługę DNS[55] - *Domain Name System*, pozwalającą na zautomatyzowane przekształcanie surowego, liczbowego zapisu adresów IP, w łatwe do zapamiętania nazwy domen, jak np. www.onet.pl. Domeny te budowane są nie tylko tak by kojarzyć się z nazwami firm, portali,

---

[52] Więcej na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Imei.

[53] Przykładowy adres MAC wygenerowany ze strony pod adresem: http://sqa.fyicenter.com/Online_Test_Tools/Test_MAC_Address_Generator.php.

[54] W tłumaczeniu Instytut Inżynierów Elektryków i Elektroników. Oficjalna strona internetowa organizacji standaryzacyjnej IEEE dostępna jest pod adresem: http://www.ieee.org.

[55] Więcej na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Domain_Name_System.

czy świadczonych usług, ale zdradzają także ogólny charakter stron – np. domeny .com oznaczają strony komercyjne, .net portale, .gov symbolizują strony rządowe, zaś .mil strony wojskowe. Usługa DNS realizowana jest przez protokół DNS funkcjonujący w najwyższej warstwie sieci – to jest warstwie aplikacji, występującej na samej górze zarówno w modelu OSI, jak i TCP/IP. Funkcjonalnie, DNS sprowadza się do stworzenia oraz udostępniania tablicy dynamicznych powiązań, które zestawiają zarejestrowane domeny sieciowe z adresami IP identyfikującymi przypisane tym domenom zakończenia sieci. Innymi słowy, DNS pozwala na określenie, z jakim adresem IP należy nawiązać połączenie, aby otworzyć stronę umieszczoną pod określoną domeną.

Przedstawiając cały mechanizm na uproszczonym przykładzie praktycznym – w polu adresowym naszej przeglądarki internetowej wpisujemy nazwę domeny strony, którą chcemy otworzyć; przeglądarka automatycznie wysyła zapytanie DNS do wybranego serwera DNS (najczęściej wskazanego automatycznie przez naszego dostawcę Internetu); serwer DNS odszukuje adres IP serwera obsługującego stronę, której domena została przesłana w zapytaniu oraz odsyła otrzymany wynik zwrotnie do naszej przeglądarki; ostatecznie, następuje realizacja połączenia ze wskazanym przez serwer DNS adresem IP. Należy zaznaczyć, że o ile znamy adres IP strony lub innego zasobu bez korzystania z pomocy usługi DNS, możemy adres ten podać od razu, pomijając opisany powyżej etap pracy przeglądarki internetowej. I tak, wpisanie w polu adresowym przywołanego wcześniej IP: 173.194.70.139, spowoduje bezpośrednie połączenie ze stroną www.google.com. Co niezwykle istotne z punktu widzenia niniejszej pracy, nieskorzystanie z usługi DNS pozwala na uniknięcie skutków jednego z najzłośliwszych ataków cybernetycznych (tzw. *cache poisoning*), polegającego na bezprawnej podmianie tablic DNS, powodującej przekierowywanie ruchu do odpowiednio spreparowanych witryn. Tak „podłożone" strony służyć mogą np. do wyłudzania danych od użytkowników przekonanych, że w istocie logują się na stronie swojego banku. Ataki skierowane przeciwko usłudze DNS należy ocenić, jako niezwykle groźne dla funkcjonowania całej sieci.

Najwyższym gestorem globalnej puli adresowej IP oraz domen najwyższego rzędu jest *Internet Assigned Numbers Authority* (IANA)[56], będąca władzą działająca w ramach *Internet Corporation for Assigned Names and Number* (ICANN)[57]. Choć organizacyjnie nadrzędna z wymienionych instytucji – ICANN, przybrała postać pozarządowej fundacji non-profit,

[56] W tłumaczeniu „Internetowa Władza Nadawania Numerów". Oficjalna strona internetowa organizacji dostępna jest pod adresem: www.iana.org.

[57] W tłumaczeniu „Internetowa Korporacja do spraw Nadawania Nazw i Numerów". Oficjalna strona internetowa organizacji dostępna jest pod adresem: www.icann.org.

otrzymała ona mocy umowy z rządem USA, który postanowił oddać Internet do sektora prywatnego, prawo do zarządzania globalną siecią. IANA z kolei, powstała pierwotnie jako grupa robocza wskazywanego już wcześniej *Internet Engineering Task Force* (IETF)[58], będącego nieformalnym forum, na którym od początku historii komercyjnego Internetu wypracowywane były standardy opisujące funkcjonowanie sieci. Zadaniem IANA było zajmowanie się właśnie zasadami adresacji.

Z czasem, gdy niezbędne stało się utworzenie instytucji, która przejęłaby ustawiczną pieczę nad rozdziałem adresów IP oraz domen, IANA stała się podstawową władzą dzielącą zasoby dostępnej puli, stając się jednocześnie autonomiczną częścią ICANN. W strukturze organizacyjnej przydziału adresów IP oraz domen, IANA oddaje poszczególne partie adresów oraz prawo rejestracji określonych domen do dyspozycji tzw. registrów, czyli podmiotów prowadzących rejestrację adresów IP oraz domen – najpierw regionalnych, a za ich pośrednictwem – lokalnych. Ostatecznie zasoby te trafiają do klientów indywidualnych najczęściej za pośrednictwem dostawców usług sieciowych, uzyskujących od registrów pule adresów IP oraz prawo rejestracji domen. Co niezwykle istotne, zgodnie z zasadami określonymi przez ICANN, przyznanie domeny dopuszczalne jest wyłącznie na czas określony, który nie może przekroczyć dziesięciu lat[59]. Wiąże się to z koniecznością okresowego odnawiania rejestracji w przypadku, gdy chce się utrzymać daną domenę. Należy zauważyć, że zamiast powszechnie używanego określenia „zakup domeny" powinno mówić się w tej sytuacji raczej o jej dzierżawie. Rolę polskiego *registry* stron internetowych w domenie .pl (np. www.onet.pl) oraz subdomen (np. .gov.pl) jest NASK – Naukowa Akademicka Sieć Komputerowa, będąca jednostką badawczo-rozwojową, powstałą pierwotnie przy Uniwersytecie Warszawskim. Aktualnym dzierżawcą domeny rządowej .gov.pl (wykorzystywanej np. przez strony www.sejm.gov.pl, czy www.kprm.gov.pl), który uzyskał czasowe prawo dysponowania nią na mocy rejestracji dokonanej w NASK, jest zaś IPPT PAN – Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk. Na zasadach partnerstwa, NASK umożliwia rejestrację domen z rozszerzeniem .pl także wielu podmiotom komercyjnym, co zapewnia odpowiedni poziom konkurencyjności na rynku rejestracji oraz obsługi domen[60].

Obok wskazanych już wyżej zadań ICANN, organizacja ta zajmuje się także

[58] W tłumaczeniu „Grupa zadaniowa inżynierii Internetu". Więcej o organizacji na jej oficjalnej stronie internetowej pod adresem: http://www.ietf.org/.

[59] Ogólne zasady rejestracji domen odnoszące się do różnych typów domen opisane są na stronie internetowej pod adresem: http://www.icann.org/en/about/learning/faqs.

[60] Dla przykładu, jednymi z najpopularniejszych podmiotów zajmujących się rejestracją domen są firmy działające poprzez portale nazwa.pl, home.pl, czy ehost.pl.

nadzorowaniem tzw. arbitrażu domenowego, prowadzonego wyłącznie przez akredytowane centra, mającego na celu z jednej strony umożliwienie polubownego rozstrzygania sporów dotyczących praw do danej domeny, zaś z drugiej, zwalczanie praktyki nieuczciwego rejestrowania domen internetowych - nazywanej *cybersquatting*. Wskazany proceder polega na wyprzedzającym rejestrowaniu domen, najczęściej całymi partiami i we wszelkich możliwych odmianach, do których nie posiada się żadnych podstaw prawnych (np. zawierających nazwę cudzej firmy, czy tytuł nowego filmu konkurencyjnej wytwórni) w celu ich późniejszej odsprzedaży z bezpodstawnym zyskiem. Na marginesie, warto w tym miejscu zauważyć, że cena pojedynczych domen może dziś sięgać setek tysięcy, a nawet milionów dolarów - np. szacunkowa wartość domeny coca-cola.com to około dwieście tysięcy dolarów, podczas gdy domena social.com została odsprzedana w 2011 r. za przeszło dwa i pół miliona dolarów (!)[61]. Jako jeden z głośnych przykładów *cybersquatting'u* wskazać natomiast można przypadek domeny madonna.com, która po przeprowadzonym przez WIPO (*World Intellectual Property Organization*[62]) postępowaniu została odebrana nabywcy oraz oddana słynnej wokalistce, Madonnie Ciccone[63]. Pozwany w sprawie domeny, Dan Parisi, biznesmen branży pornograficznej wykorzystujący domenę dla prowadzenia strony z treściami dla dorosłych, żądał od piosenkarki dwudziestu tysięcy dolarów za oddanie praw do domeny, jednak tej udało się wykazać, że rejestracja została dokonana wyłącznie w celu uzyskania bezpodstawnych korzyści majątkowych. Szacunkowa dzisiejsza wartość odzyskanej domeny oscyluje na granicy stu tysięcy dolarów.

Arbitraż domenowy, nazywany także czasami sądem domenowym, prowadzony jest w oparciu o określone przez ICANN zasady polityki UDRP[64] – *Uniform Domain Resolution Policy,* które obowiązkowo muszą być wdrażane przez wszystkich *registrów* rejestrujących domeny. Ci w efekcie przenoszą ich stosowalność na klientów końcowych wchodzących w posiadanie domen, którzy muszą wyrazić zgodę na możliwość zastosowania wobec nich zasad polityki. Pomimo szybkości oraz elastyczności arbitrażu, z uwagi na ograniczoną właściwość rzeczową prowadzonego w ramach UDRP sądu domenowego niewładnego do rozstrzygania sporów co do pewnych kategorii domen, ale także chęć stosowania przez niektóre podmioty odpowiadającego im prawa krajowego, w praktyce część sporów

61 Dane ze stron internetowych pod adresami: http://widestat.com/coca-cola.com oraz http://www.businessinsider.com/20-most-expensive-domain-names-2011-12#1-socialcom-sold-for-2600000-15.

62 Oficjalna strona internetowa organizacji dostępna jest pod adresem: www.wipo.int.

63 Sprawa została szeroko opisana przez Ch. MacDonald Newhook w: *Cybersquatters Beware!: Insiders' Tips on Winning Domain Name Disputes*, wyd. *McGraw-Hill Ryerson*, 2002 r., s. 93 i nast.

64 Więcej na stronie internetowej pod adresem: http://www.icann.org/en/help/dndr/udrp.

prowadzonych jest z pominięciem zasad UDRP - w krajowych sądach powszechnych. Zarówno wynik arbitrażu, jak i prawomocny wyrok właściwego sądu (choć w praktyce pojawiają się na tym tle problemy związane z kwestią określania właściwości miejscowej) stanowi podstawę dla przepisania przynależności domeny w odpowiednich rejestrach ICANN oraz niższych *registrów*. Pomimo niepodważalnej zasadności zwalczania praktyki nieuczciwego rejestrowania domen, należy jednak wskazać także na krytykę wysuwaną wobec dominującej pozycji podmiotów komercyjnych w pojawiających się sporach domenowych[65]. Globalizacja ochrony wszelkiego rodzaju znaków towarowych, czy identyfikacyjnych powoduje bowiem ryzyko swoistego podbicia internetu przez najsilniejsze - najbogatsze korporacje[66].

Dane dotyczące podmiotów dysponujących adresami IP oraz domenami dostępne są publicznie, poprzez sieć, m. in. za pośrednictwem usługi *whois*. Nie oznacza to jednak prostej możliwości określenia imienia i nazwiska każdego z użytkowników sieci. Należy bowiem pamiętać, że dysponentem adresu IP najczęściej nie jest osoba fizyczna – użytkownik końcowy, lecz dostawca usług sieciowych, który udziela na rzecz swojego klienta czasowej dzierżawy określonego adresu. Sprawdzając zatem dane powiązane z adresem IP takiego użytkownika otrzymujemy informacje dotyczące jego usługodawcy. W przypadku domen usługa *whois* pozwala natomiast poznać podstawowe dane o podmiocie, który dokonał rejestracji oraz serwerze, na którym fizycznie ulokowana jest strona. Do łatwego wyszukiwania wszelkich dostępnych informacji wykorzystuje się przygotowane w tym celu serwisy sieciowe, pozwalające na proste, niewymagające specjalistycznej wiedzy przeszukiwanie stosownych baz danych, jak np. www.whois.net.

Przedstawiając powyższą kwestię na gruncie praktycznego przykładu - jakie informacje można zatem ustalić na temat wybranej domeny www.rcl.gov.pl? Domena ta stanowi adres oficjalnej strony internetowej Rządowego Centrum Legislacji (należy zaznaczyć, że przedstawione dane mogą ulec zmianie nawet w krótkim czasie). Po pierwsze, sprawdzenie domeny z wykorzystaniem usługi *whois* dostarcza podstawowych informacji, że subdomena gov.pl, w ramach której funkcjonuje sprawdzany adres, pozostaje w czasowej dzierżawie NASK (uprzednio IPPT PAN), który tym samym nadzoruje też wykorzystanie

[65] Tak np. na stronie internetowej pod adresem: http://www.iusmentis.com/trademarks/udrp/.

[66] Jako słynny przykład absurdalnej polityki wskazać należy na sprawę Mike'a Rowe, który zarejestrował domenę zbudowaną w oparciu o własne nazwisko: www.mikerowesoft.com – wymawiane po angielsku podobnie do www.microsoft.com. Choć Rowe nie wskazywał na żadne związki z gigantem branży systemów operacyjnych, firma z Redmond zażądała oddania domeny, ostatecznie osiągając swój cel w zawartej ugodzie oferującej w zamian założenie innej domeny oraz zapewnienie obsługi prowadzonej pod nią strony internetowej. Więcej o sprawie na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Microsoft_vs._MikeRoweSoft.

subdomeny niższego rzędu rcl.gov.pl. Po drugie, możemy ustalić, że serwer, na którym stoi strona RCL posiada stały adres IP 46.4.59.212 (funkcja *ping*). Adres ten fizycznie zlokalizowany jest w Niemczech[67] oraz obsługiwany przez dostawcę usług internetowych Hetzner Online AG z siedzibą w Gunzenhausen w Bawarii. Po trzecie, sam serwer podłączony do zakończenia sieci o wskazanym adresie IP pozostaje w zarządzie polskiego podmiotu jskinternet.pl, zajmującego się *hostingiem*[68] stron WWW. W uproszczeniu, usługa ta polega na odpłatnym dostarczaniu powierzchni dyskowej, na której umieszcza się pliki danej strony, wraz z zapewnianiem łącza odpowiedniej przepustowości, pozwalającego na dostęp do jej zasobów z poziomu Internetu (innymi słowy jest to udostępnianie elementów infrastruktury sieciowej, na których fizycznie zlokalizowana jest strona). Jednocześnie, wskazany adres IP wykorzystywany jest przez firmę jskinternet.pl także do obsługi innych domen, m. in. autoreduta.pl, ramy aluminiowe.pl, czy groszek.net, a tym samym, bezpośrednie wpisanie go w polu adresowym przeglądarki nie spowoduje otwarcia strony RCL, zaś wyświetlenie strony ustawionej przez podmiot *hostingowy*, z uwagi na brak w samym adresie informacji precyzującej, do której konkretnie domeny próbujemy się odwołać.

W przypadku stron należących do podmiotów prywatnych, *whois* pozwala ustalić także imię i nazwisko osoby dokonującej rejestracji domeny oraz firmę i adres prowadzonej działalności gospodarczej. Warto zauważyć, że w przypadku popularnej dziś działalności opartej na zasadzie samozatrudnienia, adres przedsiębiorstwa często pokrywa się z adresem zamieszkania osoby fizycznej. Wskazane wyżej informacje, które można uzyskać nieodpłatnie, poprzez sieć na temat dowolnie wybranej domeny (nie ma tu wymogu wykazywania interesu prawnego) pozwalają zatem na nie tylko na określenie podmiotów obsługujących domenę wraz z ich podstawowymi danymi, czy danych dostawcy usług sieciowych, który dostarcza samo łącze, ale także fizyczne określenie serwerów realizujących usługę. Znajomość adresu IP pozwala wreszcie także na prześledzenie trasy, jaką pakiety danych pokonują pomiędzy serwerem ukrytym za badaną domeną, a komputerem z którego badanie to jest wykonywane. Należy ocenić, że informacje te są niezbędne z punktu widzenia prowadzenia czynności procesowych, ale także przedprocesowych, wskazując nie tylko podstawowe źródła dowodowe, ale także umożliwiając dalsze śledzenie genezy czynu bezprawnego.

[67] Na problem zagranicznej lokalizacji niektórych rządowych stron internetowych zwrócił już wcześniej uwagę Piotr Waglowski na swojej stronie internetowej pod adresem: http://prawo.vagla.pl/node/9341.
[68] Więcej o usłudze *hostingu* na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Hosting.

Biorąc pod uwagę problematykę niniejszej pracy za niezbędne uznać należy także krótkie przedstawienie zagadnień związanych z ukrywaniem faktycznego źródła ruchu sieciowego, powodującego nie tylko utrudnienia w ustaleniu sprawcy cyberprzestępstwa, ale mogącego przerzucać podejrzenia na osobę wręcz nieświadomie zamieszaną w bezprawny proceder. Problematyka ta dotyka przede wszystkim kwestii stosowania tzw. serwerów *proxy* służących do przekierowywania oraz ukrywania ruchu, wykorzystywania usług oraz sieci anonimizujacych, łączenia się z Internetem za pośrednictwem niezabezpieczonych punktów bezprzewodowych oraz przejmowania kontroli nad komputerami nieświadomych użytkowników, nierzadko stających się wbrew swojej woli częściami tzw. botnetów, będących sieciami zdalnie sterowanych maszyn (tzw. komputery *zombie)*.

Funkcjonalność serwerów *proxy*[69] polega na przekierowywaniu ruchu sieciowego poprzez dowolnie wybrany węzeł pośredniczący, pełniący rolę *proxy*. Niezależnie od położenia geograficznego, węzeł ten wykonuje polecenia ukrywającego się za nim użytkownika, maskując prawdziwe pochodzenie podejmowanych działań. Tym samym, analiza generowanego w ten sposób ruchu sieciowego wykazuje, że pakiety danych docierające do ich końcowego odbiorcy, wysyłane są nie z adresu IP faktycznego nadawcy, ale adresu IP wykorzystywanego węzła *proxy* pełniącego rolę pośrednika. Dla powiązania działań *proxy* z działaniami ich faktycznego sprawcy niezbędne jest w tej sytuacji porównanie dzienników gromadzonych na serwerze *proxy*, które pozwolą ustalić z jakiego adresu IP wysyłane były kolejne żądania operacji.

Mając na uwadze konieczność podejmowania czasochłonnych ustaleń, nierzadko wymagających nawiązywania współpracy międzynarodowej w ramach zagranicznej pomocy prawnej, stosowanie nawet tak prostego rozwiązania, może powodować realne utrudnienia w skutecznym ściganiu przestępczości. Serwery *proxy* stanowią prosty przykład tego, jak narzędzie stworzone pierwotnie do poprawy bezpieczeństwa oraz podwyższania wydajności sieci (poprzez tworzenie lokalnych kopii najczęściej pobieranych z Internetu materiałów, co ostatecznie skraca drogę pakietów) zostało z powodzeniem zaimplementowane do prowadzenia działalności przestępczej. Należy zaznaczyć, że ustalenie adresów IP otwartych, bezpłatnych serwerów *proxy* wymaga dziś jedynie wprowadzenia odpowiedniego zapytania do wyszukiwarki, zaś niezbędna konfiguracja systemu sprowadza się do kilku prostych czynności opisanych w sieci. Obok rozlicznych danych serwerów *proxy,* w sieci dostępne są także odpowiednio przygotowane strony WWW z zaimplementowanymi w sobie

[69] Więcej na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Serwer_po%C5%9Brednicz%C4%85cy.

przeglądarkami umożliwiającymi anonimowe, choć funkcjonalnie ograniczone, *surfowanie* po Internecie (po wejściu na stronę wyposażoną w odpowiedni skrypt, adresy dalszych witryn Internetowych, które chcemy otworzyć, wprowadzamy w odpowiednim polu na stronie, zmuszając obsługujący ją serwer do nawiązania odpowiedniego połączenia z jego adresu IP).

Wskazane powyżej sieci anonimizujące[70] stanowią w istocie rozwinięcie idei serwerów *proxy*, składając się z szeregu powiązanych węzłów pośredniczących. Węzły te, mogące znajdować się w najodleglejszych zakątkach świata, przekazują pomiędzy sobą generowany ruch sieciowy w zorganizowany sposób, często stosując techniki kryptograficzne, tworząc swojego rodzaju linię przekaźnikową (*wirtualne tunele*) pomiędzy faktycznym nadawcą, a ostatecznym odbiorcą pakietów danych transmitowanych za pośrednictwem sieci. Liczba kolejnych skoków po łączach potęguje przedstawione w poprzednim akapicie utrudnienia w ściganiu cyberprzestępców, zmuszając organy wymiaru sprawiedliwości do analizowania oraz śledzenia całego elektronicznego szlaku przesyłania interesujących danych. Wielość państw, które potencjalnie mogą w tej sytuacji zostać włączone w proces wykrywczy może wprowadzać dodatkowe komplikacje związane z niekompatybilnością rozwiązań prawnych przyjmowanych na poziomie krajowym. Należy w tym miejscu podkreślić niezaprzeczalną rolę harmonizacji przepisów procesowych - zagadnienia wciąż oczekującego na przyznanie mu odpowiedniej rangi na arenie międzynarodowej.

Jako jeden z najpopularniejszych przykładów sieci anonimizujących wskazać należy sieć TOR – *The Onion Router*[71], opartą na rozwiązaniach stworzonych oryginalnie na zamówienie amerykańskiej marynarki wojennej poszukującej sposobów ochrony informacji. Oferowana przez TOR funkcjonalność polega na przekierowywaniu ruchu, nazywanym tu „trasowaniem cebulowym”[72], za pośrednictwem automatycznie zestawianego szeregu węzłów pośredniczących, które udostępniane są przez samych użytkowników sieci TOR[73]. Co istotne, zarówno korzystanie z możliwości sieci, jak i utrzymywanie na własnym komputerze węzła wymagają jedynie zainstalowania prostej w obsłudze aplikacji, której pobranie oraz

---

[70] Więcej na stronach internetowych pod adresami: http://www.techopedia.com/definition/25187/anonymity-network, czy http://en.wikipedia.org/wiki/Tor_(anonymity_network). W języku angielskim - z którego analizowany termin się wywodzi, synonimicznie stosowane są określenia, m. in. „*anonymity network*” , czy „*anonymous networks*”.

[71] Więcej o sieci TOR na oficjalnej stronie internetowej projektu pod adresem: www.torproject.org, a także w: H. Erkkonen, J. Larsson, *Anonymous Networks*, praca dostępna na stronie internetowej Uniwersytetu Chalmers, pod adresem: http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/Files/onion_routing.pdf.

[72] Więcej o metodzie na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Trasowanie_cebulowe.

[73] Liczba dostępnych dziennie węzłów przekroczyła w 2012 r. poziom trzech tysięcy, źródło statystyki na stronie internetowej pod adresem: https://metrics.torproject.org/network.html.

użytkowanie pozostają całkowicie bezpłatne. Przekazywany za pośrednictwem sieci TOR ruch poddawany jest szyfrowaniu oraz prowadzony tak, by kolejne węzły otrzymywały wyłącznie dane identyfikujące węzeł poprzedzający oraz dane niezbędne do dokonania kolejnego skoku. Dzięki tak opisanej procedurze, już trzeci węzeł nie dysponuje informacjami identyfikującymi węzeł pierwszy, zaś węzeł wyjściowy (ostatni w szeregu) nie posiada żadnych danych o oryginalnym nadawcy komunikatu. Rozwiązanie to utrudnia namierzanie ruchu sieciowego niezależnie od kierunku, z którego podejmowana jest jego próba – czy to od strony nadawcy (dokąd wysyła?), czy też odbiorcy (skąd odbiera?). Każde z połączeń pomiędzy węzłami wykorzystuje odrębną parę kluczy kryptograficznych, które zabezpieczają dane o dalszych skokach. W miarę przesyłania danych pomiędzy węzłami, kolejne warstwy zabezpieczeń są usuwane - jedna warstwa na skok, ujawniając instrukcje na temat dalszego trasowania ruchu pakietu. Nawiązaniem do tego właśnie procesu, jest przyjęta dla sieci oraz stosowanej metody nazwa (paralela do zdejmowania warstw cebuli). Ostatecznie, dla dodatkowego zmniejszenia szans na skuteczną analizę ruchu sieciowego, cała trasa zmieniana jest w krótkich, około dziesięciominutowych cyklach.

Kolejnym z wymienionych sposobów ukrywania rzeczywistego źródła ruchu sieciowego jest korzystanie z niezabezpieczonych punktów dostępowych[74] (z ang. *hotspot*[75]), czyli sieci bezprzewodowych oferujących możliwość dostępu do Internetu. Sieci takie, reprezentowane najczęściej przez domowe sieci lokalne, zbudowane w oparciu o router wyposażony w moduł łączności bezprzewodowej Wi-Fi[76], umożliwiają wygodne, pozbawione kabli, współdzielenie jednego łącza internetowego na kilku komputerach. Bez odpowiedniej konfiguracji zabezpieczeń sieci, polegającej przede wszystkim na ustaleniu hasła dostępowego, sieć taka pozostaje jednak otwarta dla wszystkich znajdujących się w jej zasięgu komputerów, czyniąc ją niezwykle prostym środkiem umożliwiającym ukrycie faktycznego źródła cyberataku.

Wskazany sposób ukrywania rzeczywistego pochodzenia transmisji sprowadzić można w efekcie do podłączenia się do Internetu za pośrednictwem cudzego, niezabezpieczonego łącza bezprzewodowego, które nieświadomie udostępniane jest przez swojego abonenta nieznanemu kręgowi odbiorców. Dalsza działalność prowadzona za

---

[74] Przykład zastosowania metody opisał szerzej B. A. Howell w: J. M. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman, T. Zarsky, *Cybercrime: digital cops in a networked environment*, New York University Press, s. 95 i następne. W opracowaniu zwrócona zostaje także uwaga na opisany poniżej w akapicie *wardriving*.

[75] Więcej na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Hotspot_(WLAN).

[76] Więcej o bezprzewodowym standardzie Wi-Fi (*Wireless Fidelity*) na oficjalnej stronie internetowej organizacji Wi-Fi Alliance, pod adresem: http://www.wi-fi.org/.

pośrednictwem takiej sieci wykonywana jest zatem *de facto* na konto właściciela zakończenia sieci, które stanowić będzie źródło ewentualnego ataku. Jednocześnie, warto zaznaczyć, że przeszukiwanie otoczenia pod kątem dostępnych sieci bezprzewodowych stanowi aktualnie wbudowaną funkcję każdego systemu operacyjnego oraz możliwe jest do wykonania przy pomocy przeciętnego komputera przenośnego, czy nawet telefonu komórkowego, wyposażonych w standardową, bezprzewodową kartę sieciową.

Sieci otwarte pozostają przy tym wyraźnie oznaczone w każdej aplikacji przeszukującej eter, czyniąc określenie oraz wybranie właściwej sieci zadaniem niewymagającym żadnych umiejętności specjalistycznych. Z uwagi na powszechność Internetu, ponad stumetrowy zasięg łączności przeciętnych komercyjnych routerów wyposażonych w technologię Wi-Fi oraz wciąż zbyt niską świadomość kwestii bezpieczeństwa wielu użytkowników - znalezienie otwartego punktu dostępowego na osiedlu składającym się z kilku bloków nie stanowi trudności. Działalność polegająca na wyszukiwaniu otwartych sieci otrzymała nawet swoją oryginalną nazwę - *wardriving*[77], stając się podstawą do budowy udostępnianych w Internecie map lokalizujących niezabezpieczone sieci. W polskim porządku prawnym brak jest regulacji, które nakazywałyby osobom fizycznym zabezpieczanie łączy bezprzewodowych wykorzystywanych na własne potrzeby, jak również penalizujących wyszukiwanie lub wykorzystywanie sieci nieświadomie pozostawionych otwartymi.

Ostatnim z wymienionych sposobów ukrywania rzeczywistego źródła cyberataku, jest bezprawne przejmowanie kontroli nad komputerami innych użytkowników cyberprzestrzeni, powiązane z problematyką organizowania tzw. botnetów[78], czyli sieci *przejętych* komputerów zaprogramowanych tak, by wykonywać przesyłane im z zewnątrz polecenia. W ramach swojego funkcjonowania, skompromitowane maszyny nie tylko przekazują dalej przesyłany przez nie ruch sieciowy – działając podobnie do serwerów pośredniczących, ale mogą także samodzielnie realizować zadane im polecenia, czyniąc to w określonym czasie, niekoniecznie od razu po przejęciu kontroli. Niechciana działalność komputera jest oczywiście skrzętnie ukrywana przed jego użytkownikiem, tak by ten nie podejmował żadnych działań skierowanych na usunięcie bezprawnie wprowadzonego oprogramowania. Jednym z symptomów działania takich aplikacji w tle, może być spadek wydajności maszyny obciążanej dodatkowymi operacjami. W przypadku botnetów, ukrywanie źródła ataku uznać

---

[77] Szerzej na temat *wardriving'u* na stronach internetowych pod adresami: http://pl.wikipedia.org/wiki/Wardriving oraz http://www.pcworld.pl/news/83005/Na.pohybel.hakerom.bezpieczne.WiFi.html.

[78] Więcej na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Botnet.

można za pochodną podstawowej funkcjonalności tychże sieci, sprowadzającą się do organizowania armii podległych maszyn. Botnety mogą być następnie wykorzystywane do realizacji szeregu cyberataków, jak atak odmowy dostępu (np. poprzez wielokrotne próby otwarcia jednej strony internetowej, kierowane przez tysiące komputerów z całego świata), podsłuchiwanie transmisji, czy rozsyłanie niechcianych bądź wręcz spreparowanych (przestępnych) wiadomości – ataki te przybliżone są szerzej w następnym rozdziale.

Komputery wchodzące w skład wskazanych wyżej sieci, nazywane *botami*[79] lub też komputerami *zombie*[80], włączane są do jej szeregów nie tylko wbrew woli, ale także bez wiedzy ich uprawnionych użytkowników, poprzez infekcję komputerów złośliwym oprogramowaniem, które może być ukryte w zasadzie w dowolnym zasobie sieciowym, w szczególności zaś w nielegalnych, pirackich kopiach oprogramowania, czy utworów artystycznych. Ta sama metoda może oczywiście służyć do przejęcia kontroli nad pojedynczym komputerem, który z racji swojej określoności (napastnik obiera za cel konkretną maszynę) może stać się także przedmiotem ściśle ukierunkowanych ataków hackerskich mających na celu złamanie zabezpieczeń systemu lub wykorzystanie odkrytych luk bezpieczeństwa. Należy podkreślić, że organizowanie botnetów wymaga nie tylko specjalistycznej wiedzy oraz nakładu prac, ale także odpowiednich środków finansowych, czyniąc sieci *zombie* narzędziem stosowanym do realizacji celowych ataków, ukierunkowanych na określone efekty lub korzyści, mogących przybierać nawet postać cyberterroryzmu. Co więcej, już zorganizowane botnety mogą także stać się przedmiotem sprzedaży lub najmu na rzecz grup przestępczych, stając się swojego rodzaju bronią. Za przykład siły, jaką dysponują rozległe sieci *botów* wskazać można wydarzenia, które miały miejsce w Estonii w 2007 r., gdy ofiarą zmasowanego cyberataku padła m. in. rządowa infrastruktura sieciowa oraz internetowe serwisy bankowe. Źródła ataku wiązane były z władzami Rosji[81].

Do rozbitego przez funkcjonariuszy FBI botnetu *Mariposa*, wykorzystywanego do nielegalnego pozyskiwania haseł bankowych oraz danych osobowych, zgodnie z szacunkami należało od ośmiu do dwunastu milionów zarażonych komputerów rozrzuconych po całym

---

[79] W języku informatycznym, słowo *bot* oznacza zautomatyzowany program, który zachowuje się niczym robot, z tą różnicą, że działa w cyberprzestrzeni. Tak np. internetowe słowniki języka specjalistycznego dostępne pod adresami: http://www.techterms.com/definition/bot, czy http://www.pcmag.com/ encyclopedia_term/0,2542,t=bot&i=38865,00.asp.

[80] Tak np. na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Zombie_(computer_science).

[81] Szerzej o wydarzeniach w Estonii na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia.

globie[82]. Pochodzący ze Słowacji, zaledwie 23 letni, autor nielegalnego oprogramowania służącego do organizacji, utrzymania oraz kontroli botnetu, przed aresztowaniem sprzedał przygotowane przez siebie aplikacje cyberprzestępcom z całego świata. Skuteczne zwalczanie oraz wykrywanie przestępstw popełnianych z zastosowaniem botnetów wymaga ze strony organów wymiaru sprawiedliwości podejmowania działań zakrojonych na skalę równie wielką, co działalność takich sieci. O ile jednak cyberprzestępcy nie zważają na obowiązujące regulacje prawne, o tyle właściwe podmioty powołane do ścigania przestępstw muszą działać z zachowaniem swojej krajowej jurysdykcji, poważnie ograniczającej szybkość, a w efekcie także skuteczność działania.

Podstawowym źródłem dowodowym pozwalającym cyberśledczym na odkrycie faktycznego źródła ataku są wcześniej wskazane logi (dzienniki) prowadzone przez operatorów sieci telekomunikacyjnych. Zestawienie odpowiednich wpisów pochodzących z serwerów pośredniczących w wymianie danych, dodatkowo precyzyjnie wysegregowanych w ujęciu czasowym, pozwala na kojarzenie wirtualnych szlaków, którymi faktycznie podążały pakiety danych interesujące właściwe organy procesowe. Tym samym, szczegółowe badanie logów umożliwia wyszkolonym technikom dochodzenie - po nitce do kłębka, do rzeczywistego sprawcy cyberprzestępstwa. Obok logów, istotnych dowodów dostarczyć może oczywiście także analiza działania oprogramowania złośliwego, które ewentualnie zostało użyte w celu realizacji przestępstwa, ale także wszelkich innych informacji uzupełniających *modus operandi* sprawcy, czy nawet pojawiających się poszlak – zwalczania cyberprzestępczości nie należy bowiem zamykać w świecie cyberprzestrzeni (np. ujawniony w domenie cyfrowej numer konta może być powodem decyzji o podjęciu dalszych działań mających na celu ustalenie danych właściciela konta, co w efekcie zaprowadzi do adresu zamieszkania, gdzie zlokalizowany może być komputer zawierający istotne dowodowo dane).

Zamykając sieciową część niniejszego rozdziału, odnotowania wymaga wreszcie także kwestia wykorzystywania w sieci zabezpieczeń kryptograficznych, służących do szyfrowania przekazywanych pomiędzy komputerami treści. W kontekście tematu pracy, zagadnienie to pozostaje w ścisłym związku zarówno z problematyką podejmowania czynności przedprocesowych, jak i procesowych, ale także kluczowym dla skuteczności całego procesu karnego postępowaniem dowodowym. Aktualnie kryptografia stosowana jest już standardowo do zabezpieczania haseł dostępowych umożliwiających korzystanie z różnych usług, składania podpisu elektronicznego, zapewniania bezpieczeństwa wrażliwych transmisji –

[82] Dane z oficjalnego oświadczenia FBI, dostępnego na stronie internetowej pod adresem: http://www.fbi.gov/news/pressrel/press-releases/fbi-slovenian-and-spanish-police-arrest-mariposa-botnet

np. związanych z dokonywaniem transakcji finansowych, czy wreszcie sieci bezprzewodowych emitujących pakiety danych w eter – umożliwiając ich niezauważalne przechwycenie. Z uwagi na rosnący poziom zagrożeń w sieci, kryptografię coraz częściej stosuje się także do ochrony poufności informacji korporacyjnych, a nawet prywatnych danych. Popularne komunikatory sieciowe (jak np. *Skype*) posiadają zaimplementowane rozwiązania szyfrujące w celu ochrony konstytucyjnie gwarantowanej tajemnicy korespondencji. Ta ochrona może być jednak również wykorzystywana w celach przestępnych, do ukrywania dowodów bezprawnej działalności.

Kontrola zaszyfrowanego ruchu, zlokalizowana na trasie zabezpieczonych pakietów danych, nie pozwala na proste odczytanie treści przekazywanych w formie tzw. szyfrogramu, lecz wymaga prowadzenia specjalistycznego dekryptażu, zabierającego śledczym cenny czas – będący nierzadko jednym z najistotniejszych czynników warunkujących skuteczność postępowania. Niezwykle kontrowersyjne rozwiązanie przedstawionego problemu zaprezentowały Niemcy zamawiając, w ramach kontraktu rządowego, oprogramowanie szpiegujące służące do włamywania się do komputerów osób podejrzanych w celu podsłuchiwania danych przetwarzanych bezpośrednio na ich komputerze (a więc jeszcze przed zaszyfrowaniem lub po odszyfrowaniu). Oprogramowanie określone zostało przez społeczność internetową mianem *Bundestrojaner*[83], nawiązującym do tzw. koni trojańskich będących rodzajem oprogramowania złośliwego. Brak wyraźnych podstaw prawnych do prowadzenia tego typu działań przez właściwe służby państwowe stał się zalążkiem ogólnoświatowej debaty na temat praw człowieka i obywatela w sieci – problemy te zaprezentowane są szerzej w kolejnych rozdziałach pracy.

Kryptografię podzielić można na symetryczną oraz asymetryczną, w zależności od tego, czy do szyfrowania i odszyfrowywania danych stosuje się jeden klucz, czy dwa różne. Z uwagi na znaczenie szyfrowania dla bezpieczeństwa państwa, obrót technologiami kryptograficznymi podlega istotnym ograniczeniom oraz reglamentacji[84], których standardy w przypadku obszaru Europy narzucone zostały przez prawodawstwo Unii Europejskiej. Popularnym standardem kryptograficznym wykorzystywanym w oferowanych komercyjnie urządzeniach sieciowych umożliwiających bezprzewodową łączność opartą na technologii

[83] Analizę zdobytego kodu oprogramowania przeprowadziła grupa CCC (*Chaos Computer Club*). Więcej na ten temat na stronach internetowych pod adresami: http://www.ccc.de/en/updates/2011/staatstrojaner , oraz http://de.wikipedia.org/wiki/Online-Durchsuchung.

[84] W polskim porządku prawnym funkcje te realizują przepisy ustawy z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (Dz. U. Nr 67, poz. 679, z późn. zm.) oraz wydane na jej podstawie akty wykonawcze.

Wi-Fi, jest AES (*Advanced Encryption Standard*)[85] wykorzystujący symetryczny algorytm *Rijndael*. AES stanowi element powszechnie przyjętego standardu bezpieczeństwa sieci bezprzewodowych WPA2 (*Wi-Fi Protected Access 2*)[86].

Przy okazji przybliżania zabezpieczeń kryptograficznych warto zwrócić uwagę także na inny sposób zabezpieczania poufności przekazywanych informacji, jakim jest stosowanie tzw. technik steganograficznych[87], znanych już od przeszło dwóch tysięcy lat. W odróżnieniu od kryptografii, steganografia polega nie tyle na ochronie treści, co ukrywaniu samego faktu istnienia komunikatu – np. poprzez nanoszenie na pismo niewidocznych na pierwszy rzut oka znaków wodnych, czy wprowadzanie przekazów budowanych z wybranych liter określonych wyrazów. Ukryte wiadomości mogą być wprowadzane oczywiście zarówno do dokumentów przybierających formę pisemną, jak i dowolnych innych materiałów: graficznych, dźwiękowych, czy kodu binarnego plików – w tym przykładowo programów lub stron internetowych. Odczytanie ukrytej wiadomości wymaga oczywiście wcześniejszego przyjęcia określonego sposobu interpretacji treści wybranego „nośnika", zaś przemycane przekazy mogą chować się w jego najdrobniejszych niuansach, nie posiadając żadnych cech szczególnych, które zwracałyby uwagę osób postronnych. Stosowanie steganografii – tak, jak kryptografii, stanowić może kolejny sposób ukrywania ewentualnych dowodów popełnienia przestępstwa. Steganografia może być dodatkowo wspierana rozwiązaniami kryptograficznymi (ukrywanie wcześniej zaszyfrowanego komunikatu).

Ch o ćw tym miejscu jedynie sygnalizacyjnie, warto od razu podkreślić, że na tle wskazanych powyżej sposobów ukrywania rzeczywistych źródeł cyberataków, obok licznych kwestii procesowych – głównie dowodowych, rysuje się także szereg zagadnień z dziedziny prawa karnego materialnego, związanych przede wszystkim z problematyką oceny oraz przypisywania winy, ale także określania formy popełnienia przestępstwa (np. niesprawczej formy zjawiskowej, jaką jest pomocnictwo). Zagadnienia te poruszane są w kolejnym rozdziale opisującym poszczególne rodzaje ataków, jakie mogą występować w cyberprzestrzeni.

---

[85] Więcej na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Advanced_Encryption_Standard.
[86] Więcej na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/IEEE_802.11i-2004.
[87] Więcej na stronach internetowych pod adresami: http://www.sans.org/reading_room/whitepapers/stenganography/steganography-past-present-future_552, oraz http://pl.wikipedia.org/wiki/Steganografia.

§3. Wybrane zagadnienia związane z budową oraz wykorzystywaniem informatycznych nośników danych

Wskazany w pierwszej części rozdziału wzrost mocy obliczeniowej komputerów stał się motorem dla równoległego, równie szybkiego rozwoju informatycznych nośników danych. Zarówno pojemność, jak i szybkość nowoczesnych nośników musiały bowiem zostać dostosowane do nowych wymagań, tak, by nie wytwarzać tzw. wąskich gardeł (z ang. *bottlenecks*), czyli elementów sprzętowych, powodujących obniżenie wydajności całego systemu. Innymi słowy, by procesor mógł przetworzyć dane musi dostać odpowiednią ilość danych wejściowych, zaś wygenerowane efekty muszą zostać równie szybko odebrane oraz zapisane w odpowiedniej pamięci (RAM – podręcznej; lub ROM – służącej do stałego magazynowania danych). Stosowane niegdyś dyskietki (tzw. *flopy disks)* mieszczące niespełna półtora megabajta danych (dokładnie 1440 kilobajtów – w przypadku dyskietki 3,5 cala) dziś nie wystarczają już nawet do przeniesienia sformatowanego dokumentu tekstowego. Zastąpiły je płyty CD, DVD oraz Blu-Ray, a także szeroko stosowane pamięci półprzewodnikowe. Standardem stają się dyski twarde o pojemności przekraczającej 500 gigabajtów danych.

Na wstępie, należy zaznaczyć, że stosowane do określania ilości danych przedrostki dziesiętne (kilo-, mega-, giga-, itd.) wprowadzają istotną nieścisłość do przyjętej terminologii. Choć formalnie jeden kilobajt powinien równać się 1.000 bajtów (8.000 bitów), w informatyce operującej w systemie binarnym, potoczne wyrażenie „kilobajt” odnosi się w rzeczywistości do 1024 bajtów (2^{10}). Analogicznie, wyrażenie „megabajt” stosowane jest w przyjętej praktyce na oznaczenie nie miliona bajtów, lecz 1.048.576 (2^{20}). Należy podkreślić, że wraz ze wzrostem mnożników, powiększa się błąd pomiędzy stosowanym w praktyce nazewnictwem, a rzeczywistą ilością danych, który przyjęty został przed laty rozmyślnie, jako uproszczenie niepowodujące istotnego błędu, z uwagi na niewielkie ilości przetwarzanych danych. Niegdyś marginalne odchylenie, w dobie przetwarzania terabajtów danych stało się jednak istotnym zagadnieniem. Proponowanym przez społeczność informatyczną rozwiązaniem przedstawionego problemu jest zastąpienie przedrostków dziesiętnych, przedrostkami binarnymi (kibi-, mebi-, gibi-, itd.), które pozwalałyby w sposób precyzyjny określać porcje danych[88]. Przyjęte nawyki skutecznie blokują jednak wprowadzenie zmian w nazewnictwie, powodując wiele błędów wynikających z niedoprecyzowywania wykorzystywanych pojęć.

---

[88] Więcej na ten temat na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Megabajt.

Przedstawiając krótką typologię informatycznych nośników danych, należy podzielić je na nośniki magnetyczne, optyczne oraz półprzewodnikowe[89]. Do nośników magnetycznych zalicza się dyski twarde (HDD) oraz wycofywane dziś z użytku dyskietki (FDD); nośniki optyczne to wszelkiego rodzaju płyty – CD, DVD, HD-DVD, czy popularne jako nośnik filmów płyty Blu-Ray[90]; przykładem pamięci półprzewodnikowych są zaś pamięci typu *flash* stosowane najczęściej w przenośnych pamięciach *pendrive*, czy dyskach SSD (*Solid State Drive*) częściowo zastępujących rolę dysków twardych. Nośniki magnetyczne oraz optyczne nazywane są także niekiedy „nośnikami mechanicznymi", jako że ich wykorzystanie wymaga zastosowania odpowiednich urządzeń mechanicznych (np. napęd płyt DVD, czy silnik talerza oraz głowica w przypadku dysków twardych). Pamięci półprzewodnikowe pozbawione są w odróżnieniu wszelkich elementów ruchomych, czego efektem jest skrócenie ich czasu reakcji, wyższa odporność na wstrząsy, a także obniżone zużycie energii. Innym podziałem, nie odnoszącym się ściśle do wykorzystywanego medium, jest rozdział nośników na jedno- oraz wielokrotnego zapisu. Nośniki jednokrotnego zapisu, po umieszczeniu na nich danych, nie mogą być z nich czyszczone, ani nadpisywane, zostawiając nieusuwalny ślad danych. Przykładami takich nośników są przede wszystkim nośniki optyczne, choć należy podkreślić, że występują one także w wersjach wielokrotnego zapisu (oznaczone skrótami CD-RW, DVD-RW, BD-RW[91]). Każdy ze wskazanych nośników posiada oczywiście swoją specyfikę techniczną, której poznanie oraz wykorzystanie przez przedstawicieli wymiaru sprawiedliwości stanowi jeden z istotnych warunków skutecznego ścigania karnego. Odnośnymi zagadnieniami przedstawianymi w niniejszej części rozdziału, w ujęciu zarówno technicznym, jak i prawnym, zajmuje się wyodrębniona dziedzina kryminalistyki, nazywana informatyką śledczą (z ang. *computer forensics*).

Niezależnie od zastosowanego nośnika, przechowywane na nim dane informatyczne zapisywane są zawsze w postaci binarnej (bit po bicie), tworzącej w całości tzw. obraz nośnika. W obrazie tym odnaleźć można także dane, które zapisane są na ukrytych partycjach, niewidocznych z pozycji zwykłego użytkownika nośnika. Magazynowany na wszelkich nośnikach zapis binarny interpretowany jest dzięki kolejnym warstwom oprogramowania jako

---

[89] Na podstawie m. in.: A. Reyes, J. Wiles, *The Best Damn Cybercrime and Digital Forensics Book Period,* Syngress 2007, s 41 i nast. oraz Mi Cross, D. Littlejohn Shinder, op. cit., s. 128 i nast.

[90] Jako ciekawostkę należy wskazać, że technologia niebieskiego lasera wykorzystywana do zapisu oraz odczytu płyt Blu-Ray została opracowana przy wydatnym wkładzie polskich naukowców pracujących w Instytucie Wysokich Ciśnień PAN oraz Wojskowej Akademii Technicznej, tak np. na stronach internetowych pod adresami: http://pl.wikipedia.org/wiki/Blu-ray oraz http://finanse.wp.pl/gid,13303958,opage,3,galeria.html?ticaid=1e1cf.

[91] Skrót RW pochodzi od anglojęzycznego wyrazu *rewriteable* – w dosłownym tłumaczeniu „ponownie zapisywalny".

pliki, które posiadają swoją nazwę, wskazujące na rodzaj pliku rozszerzenie (np. .doc - dokument, .avi - film, .mp3 - nagranie dźwiękowe, .exe - wykonywalny program, itd.) oraz treść. W efekcie, w przypadku fizycznego uszkodzenia nośnika, np. poprzez przebicie talerza dysku twardego, czy głębokie uszkodzenie poliwęglanowej warstwy nośnej płyty CD[92] - uniemożliwiających standardowy odczyt zapisanych danych, wciąż możliwe jest odzyskanie fizycznie nieuszkodzonego fragmentu obrazu. Wymaga to zastosowania specjalistycznych rozwiązań zarówno sprzętowych, jak i programowych, pozwalających nie tylko odczytać odzyskane bity informacji, ale także dzielić je na poszczególne pliki, co w przypadku uszkodzenia struktury logicznej plików może wymagać przeprowadzenia analizy danych. Warto zaznaczyć, że dane przechowywane na dysku twardym podlegają procesowi defragmentacji, czyli naprzemiennego zapisywania fragmentów różnych plików.

Defragmentacja jest wynikiem optymalizacji pracy dysku twardego, który zapisuje otrzymywane strumienie danych budujących różne pliki w możliwie najkrótszym czasie, a więc bez ciągłego przemieszczania głowicy pomiędzy obszarami, które byłyby specjalnie wydzielane dla poszczególnych materiałów. W przypadku uszkodzenia struktury plików pomieszane w ten sposób bity nie podlegają automatycznemu rozdziałowi pomiędzy pliki, powodując w efekcie konieczność ponownego przypisywania poszczególnych bitów do tworzonych przez nie oryginalnie plików. Obok defragmentacji, utrudnieniem dla rekonstrukcji, ale także samego odnajdywania danych celem ich zabezpieczenia może być także wykorzystywanie tzw. macierzy dyskowych wykorzystujących technologię RAID (*Redundant Array of Independent Disks*)[93], pozwalających na funkcjonalne scalanie wielu dysków twardych w jeden wspólny obszar logiczny, bądź to w celu przyspieszenia pracy (dwa lub więcej dysków zapisujących dane równolegle), bądź dla poprawy bezpieczeństwa danych (m. in. poprzez nagrywanie lustrzanych kopii bezpieczeństwa). Znajomość stosowanych w tym zakresie rozwiązań technicznych uznać należy za niezbędną dla prowadzenia skutecznych czynności dochodzeniowo-śledczych. Zabezpieczenie jedynie części macierzy może bowiem powodować pozyskanie jedynie fragmentów istotnych dla celów dowodowych plików, które w oderwaniu od reszty danych mogą być pozbawione jakiejkolwiek wartości procesowej.

Zbierane w celach procesowych dane muszą przede wszystkim zachowywać swoją pełną integralność – a więc dawać gwarancję, że nie zostały w żaden sposób zmodyfikowane.

---

[92] Więcej o budowie dysku twardego na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Dysk_twardy. O budowie płyty CD zaś: http://pl.wikipedia.org/wiki/P%C5%82yta_kompaktowa.

[93] Więcej na temat RAID oraz różnych jego poziomów na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/RAID.

Twierdzenie to stanowi jedną z naczelnych zasad informatyki śledczej[94], bowiem wykrycie i zabezpieczenie nawet najpełniejszych, najgłębiej skrywanych dowodów winy pozostanie bez znaczenia dla wyniku postępowania, o ile pozyskanie materiału wywoła podejrzenia, co do możliwości jego zniekształcenia lub wręcz przekształcenia. Nieumiejętne obchodzenie się z dowodami cyfrowymi może przekreślić ich wartość procesową w ciągu zaledwie jednego kliknięcia, czyniąc z nich niezwykle delikatne źródło. Należy bowiem podkreślić, że nawet zwykłe włączenie komputera może powodować pojawienie się w plikach systemowych informacji o dacie ostatniego logowania, będącej samą w sobie zmianą oryginalnego zapisu. Podobnie otwarcie pliku może poprzez nieuwagę spowodować zmianę zapisu daty jego ostatniej modyfikacji, która to zmiana będzie wykorzystywana do obalenia odnalezionych dowodów. By zapobiec modyfikacjom danych zapisanych na procesowo zabezpieczonych nośnikach, nośniki te muszą być zarówno pozyskiwane, jak i analizowane przez odpowiednio przeszkolonych techników przy zastosowaniu specjalistycznego sprzętu oraz oprogramowania, gwarantujących wskazaną wyżej integralność danych, a w efekcie niepodważalność uzyskanego materiału dowodowego.

Podobnie, jak ma to miejsce przy przesyłaniu pakietów danych za pośrednictwem sieci, informacje przechowywane na informatycznych nośnikach mogą być zapisywane w postaci zaszyfrowanej, uniemożliwiającej ich prosty odczyt. Zabezpieczone w ten sposób dane, choć przez cały czas dostępne, nie posiadają żadnej wartości do momentu ich odszyfrowania. Czas niezbędny do jego przeprowadzenia pozostaje oczywiście w stosunku wprost proporcjonalnym do wydajności zastosowanych środków dekryptażu oraz odwrotnie proporcjonalnym do wielkości odszyfrowywanego obszaru. Kodowaniu podlegać mogą tak pojedyncze pliki, jak i całe partycje dyskowe. Analogicznie, jak w przypadku szyfrowania transmisji sieciowych, należy twierdzić, że szyfrowanie będące rozwiązaniem mającym pierwotnie na celu zapewnienie poufności i bezpieczeństwa danych, tak by nie wpadły w niepowołane ręce, może być wykorzystywane także przez cyberprzestępców do prób ukrywania lub zacierania dowodów prowadzonej działalności. Stosowanie rozwiązań kryptograficznych w takich przypadkach stanowi jeden z problemów, których rzeczywiste rozwiązanie musi wiązać się z przyjęciem regulacji prawnych o charakterze międzynarodowym.

Podnosząc kwestię nośników danych, warto zwrócić uwagę także na najświeższą

[94] Tak np.: A. Reyes, J. Wiles, op. cit., s. 54 i nast.

problematykę wykorzystywania tzw. chmur (z ang. *cloud computing*)[95]. W skrócie, chmurą nazywana jest gotowa platforma sprzętowa, bądź sprzętowo-programowa, której zasoby udostępniane są odpłatnie klientom chmury. Dzięki takiemu rozwiązaniu, użytkownicy chmur nie muszą fizycznie posiadać kosztownych, nowoczesnych komputerów, ani najnowszego oprogramowania by móc z nich korzystać. Po stronie użytkowników wystarczające jest posiadanie terminali dostępowych, za pośrednictwem których kontrolują oni wynajęte elementy chmury. Rozwiązanie to pozwala efektywnie wykorzystywać zasoby chmury redukując koszty ponoszone przez poszczególnych jej beneficjentów przy jednoczesnym zapewnieniu im dostępu do najnowocześniejszych rozwiązań. Jedną z najpopularniejszych funkcjonalności chmur jest udostępnianie powierzchni dyskowych, umożliwiających bezpieczne magazynowanie ogromnych ilości danych oraz ich szybką dystrybucję, np. pomiędzy oddziałami przedsiębiorstwa. Dane przetwarzane w chmurach fizycznie zlokalizowane mogą być w dowolnych punktach świata, wszędzie tam, gdzie rozmieszczona jest infrastruktura podbudowującą chmurę. W efekcie stosowania chmur, fizyczne zabezpieczenie nośników wykorzystywanych do gromadzenia danych – wykorzystywanych przez podmiot krajowy, może wiązać się z koniecznością podejmowania czasochłonnej współpracy międzynarodowej w ramach pomocy prawnej. Jednocześnie, fakt współużytkowania jednej przestrzeni dyskowej z innymi podmiotami będącymi klientami tej samej chmury, może powodować komplikacje oraz dalsze trudności techniczne w niezwłocznym pozyskiwaniu należycie zabezpieczonych nośników danych, spełniających standardy niezbędne dla wykorzystania uzyskanych materiałów w procesie karnym.

PODSUMOWANIE

Przedstawione w niniejszym rozdziale zagadnienia stanowią istotne poszerzenie kontekstu definicji pojęcia cyberprzestrzeni, jednocześnie istotnie podbudowując dalsze rozważania dotyczące nowoczesnych form przestępczości popełnianej w cyberprzestrzeni. Zarówno bowiem opisanie *modus operandi* działania sprawców poszczególnych rodzajów cyberprzestępstw (opisywanych szeroko w kolejnym rozdziale), jak i przeprowadzenie ich rzetelnej analizy prawnej – zarówno w ujęciu materialnym, jak i procesowym, wymagają prowadzenia odnośnych rozważań na tle zasad, w oparciu o które zbudowane jest oraz funkcjonuje specyficzne środowisko cyfrowej domeny. Co zasługuje na podkreślenie -

[95] Więcej na temat chmur oraz ich rodzajów na stronie internetowej pod adresem: http://www.microsoft.eu/cloud-computing/?gclid=CMnn9siv8a4CFUZa3wodLSU-Hg.

środowisko to stanowiąc z jednej strony teatr działań cyberprzestępców, z drugiej jest równolegle obszarem poszukiwań oraz pracy cyberśledczych. Zawarta w niniejszym rozdziale analiza pozwala zwrócić szczególną uwagę na następujące kwestie:

- komputery to urządzenia zbudowane z szeregu połączonych podzespołów, których poznanie pozwala zrozumieć podstawowe zasady przetwarzania danych zapisanych w postaci cyfrowej – stanowiących budulec cyberprzestrzeni,
- na najniższym poziomie logicznym komputery przetwarzają binarne ciągi zbudowane wyłącznie z zer i jedynek,
- ciągi te składają się na funkcje, wyrazy, zdania, a także złożone formy graficzne, czy dźwięk dzięki zastosowanemu oprogramowaniu, które kieruje pracą komputera. Poprawne zrozumienie tego, co komputer naprawdę wykonuje – oraz jak to robi, wymaga zatem bliższego poznania zainstalowanego na nim oprogramowania,
- specjalistyczna wiedza dotycząca pracy komputera, czy elementów infrastrukturalnych sieci komputerowych, pozwala nie tylko badać rzeczywiste działania poszczególnych maszyn oraz ich komponentów, ale także wpływać na nie,
- należy mieć na uwadze, że nie wszystkie aplikacje muszą działać w sposób jawny powodując widoczne dla użytkownika efekty. Każde zabezpieczenie systemowe chroniące komputer przed utratą nad nim kontroli może być ominięte lub złamane, tak jak każdy, nawet najmocniejszy zamek,
- podstawy budowy oraz zasad funkcjonowania nowoczesnych sieci komputerowych, w szczególności zaś Internetu, stanowią elementy niezbędne dla dalszego przedstawienia oraz zrozumienia zjawiska cyberprzestępczości. To, czym są pakiety danych, jaką rolę pełni adres IP identyfikujący zakończenie sieci wykorzystywane w procesie wymiany danych, adres MAC określający konkretne urządzenie końcowe, czy wreszcie w jaki sposób zestawiane jest logiczne łącze pomiędzy dwoma dowolnie obranymi zakończeniami sieci w ramach procesu trasowania, pozwala na wprowadzenie niezbędnych pojęć, służących tak do opisu występujących w cyberprzestrzeni ataków, jak i metod stosowanych do ich wykrywania. Budowa oraz funkcjonowanie globalnej sieci pozwala wreszcie także na pełne umocowanie kwestii współpracy międzynarodowej w zakresie zwalczania przestępczości internetowej,
- funkcjonowanie sieci uzupełniają rozważania dotyczące roli oraz zasad przydziału domen, przybliżające jednocześnie organizację Internetu,

- jedną z cech charakteryzujących działanie cyberprzestępców jest ukrywanie swojej tożsamości, które realizowane może być z wykorzystaniem szeregu metod, niekoniecznie wymagających włamywania się do komputerów innych użytkowników. Obok stosowania serwerów pośredniczących (*proxy*), czy sieci anonimizujących, niezwykle skuteczne oraz proste jest wykorzystywanie niezabezpieczonych punktów bezprzewodowych, pozwalających łączyć się z Internetem pod przykryciem tożsamości osoby, która nieświadomie udostępnia swoje łącze,
- udostępniane w sieci zasoby, w szczególności zaś dystrybuowane darmowo nielegalne kopie oprogramowania, czy materiałów objętych ochroną praw autorskich, mogą powodować infekcję komputerów złośliwym oprogramowaniem powodującym możliwość przejęcia częściowej kontroli na komputerem przez osoby trzecie. Działalność taka może w efekcie posłużyć do organizowania całych sieci podległych maszyn, nazywanych botnetami. Sieci takie mogą być wykorzystywane niczym armie do realizacji określonych ataków,
- wiedza na temat budowy oraz funkcjonowania komputerów oraz sieci stanowi punkt wyjścia dla określenia źródeł dowodów przestępstw popełnianych w obszarze cyberprzestrzeni. Ich poprawne zabezpieczenie również uwarunkowane jest znajomością zasad, w oparciu o które przetwarzane są cyfrowe dane. Obok typologii dostępnych rodzajów nośników danych, w rozdziale przedstawione zostały także kwestie stosowania macierzy dyskowych oraz zdobywających coraz większą popularność chmur,
- istotnym zagadnieniem – zarówno w ujęciu karno-materialnym, jak i procesowym, jest także wreszcie wykorzystywanie zabezpieczeń kryptograficznych, które obok ochrony poufności danych, mogą być wykorzystywane również do ukrywania śladów działalności cyberprzestępców.

Rozdział IV
Systematyka oraz kwalifikacja prawna wybranych cyberprzestępstw

§1. Cyberprzestępstwa w zakresie transmisji danych w sieci

Opierając się na wcześniejszych rozważaniach dotyczących definicji zjawiska cyberprzestępczości, niniejszy rozdział poświęcony został przeprowadzeniu bliższej analizy konkretnych, wybranych cyberprzestępstw. Analiza taka pozwala nie tylko na przybliżenie najpowszechniejszych przestępstw cyberprzestrzeni, ale także w sposób istotny uzupełnia dotychczasowe rozważania, rozbudowując obraz tego, czym naprawdę jest cyberprzestępczość i na czym polega jej związek z cyberprzestrzenią. Samo pojęcie „cyberprzestępstwa" rozumiane jest tu w sposób ujęty w podsumowaniu części definicyjnej.

W efekcie przyjętej budowy, oprócz zagadnień definicyjnych dot. pojęcia cyberprzestępczości, niniejszy rozdział w sposób istotny wykorzystuje także wszelkie wcześniejsze rozważania dotyczące obszaru cyberprzestrzeni - jako domeny w której popełniane są cyberprzestępstwa. W szczególności, istotną rolę pełnią tu wiadomości o charakterze technicznym, które przedstawione zostały w rozdziale III. Wiadomości te pozwalają na wprowadzenie szerszej niż tylko prawniczej perspektywy spojrzenia na zjawisko cyberprzestępczości, umożliwiając przybliżenie technicznej strony *modus operandi* sprawców poszczególnych cyberataków oraz nadanie kontekstu faktycznego prowadzonym tu rozważaniom teoretycznym.

W ramach charakterystyki poszczególnych cyberprzestępstw opisane zostały zarówno metody ich popełniania (rodzaje cyberataków), dobra prawnie chronione będące przedmiotem zamachu, jak również potencjalne kwalifikacje prawne czynów, dokonywane na gruncie obowiązującego w Polsce Kodeksu karnego. Przedstawiony w rozdziale katalog działań przestępnych komponowany był z myślą o możliwie szerokim zaprezentowaniu niezwykle różnorodnego zjawiska, jakim jest cyberprzestępczość - stąd też w katalogu tym uwzględnione zostały nie tylko czyny, w których bezprawne działanie polega wyłącznie na wykonywaniu zaawansowanych operacji o charakterze technicznym, podejmowanych

wewnątrz cyberprzestrzeni[1], ale także czyny łączące nowoczesne formy i metody z działaniami *tradycyjnymi*, dla których systemy teleinformatyczne stanowią rodzaj szczególnego narzędzia[2]. Jako przykład wskazać można tu tzw. inżynierię społeczną, będąca jednym z narzędzi wykorzystywanych w przestępstwie *phishingu*.

Z uwagi na specyfikę cyberprzestępczości, powodującą, że jeden określony czyn może zostać skierowany przeciwko wielu różnym (często całkowicie różnorodnym) dobrom prawnie chronionym, analizowane w niniejszym rozdziale cyberprzestępstwa zostały skategoryzowane wedle nowego, autorskiego podziału, w którym odwołano się do budowy cyberprzestrzeni oraz nakreślonej w rozdziale III drogi, jaką pokonują pakiety danych w trakcie transmisji pomiędzy systemami. Drogę tę, w ogromnym uproszczeniu, można scharakteryzować jako: wysłanie danych przez nadawcę, trasowanie danych pomiędzy kolejnymi węzłami sieci, dostarczenie oraz wpuszczenie danych bądź na serwer sieciowy (np. celem zamieszczenia danych na stronie WWW), bądź do systemu adresata (np. przy bezpośrednim przesyłaniu plików w P2P[3]), oraz ostatecznie ich przetworzenie w zaprogramowany sposób u odbiorcy. Ścieżkę tę uzupełnia ewentualne przygotowywanie narzędzi służących do popełnienia cyberprzestępstwa, w tym organizowanie sieci tzw. *botnetów*. W efekcie, poszczególne cyberprzestępstwa podzielone zostały na następujące kategorie:

I. cyberprzestępstwa w zakresie transmisji danych w sieci;
II. cyberprzestępstwa związane z upublicznianiem, udostępnianiem lub rozsyłaniem określonych treści lub materiałów;
III. cyberprzestępstwa związane z uzyskaniem nieuprawnionego dostępu do systemu;
IV. cyberprzestępstwa związane z dokonywaniem nieuprawnionych czynności wewnątrz systemu, w tym odczytywanie oraz modyfikowanie jego zasobów;
V. oszustwo komputerowe.

Zaprezentowany podział nie tylko stanowi rozwiązanie nowatorskie - niezbędne z punktu

---

1 M. Kliś, Przestępczość w Internecie. Zagadnienia podstawowe, Czasopismo Prawa Karnego i Nauk Penalnych, Wydawnictwo Polska Akademia Umiejętności, Kraków 2000, opracowanie dostępne na stronie internetowej pod adresem: http://prawo.vagla.pl/node/905.

2 B. Fischer, Przestępstwa komputerowe i ochrona informacji. Aspekty prawno kryminalistyczne, Zakamycze, Kraków 2000, s. 25 i nast.

3 P2P - z ang. *peer to peer*, technologia przesyłania danych bezpośrednio pomiędzy systemami użytkowników, z pominięciem serwerów, które tymczasowo składują dane (zamiast drogi użytkownik A -> serwer -> użytkownik B, dane przekazywane są bezpośrednio pomiędzy użytkownikami). Poza wygodą, jaką oferuje model P2P, technologia ta stała się swoistym synonimem serwisów oferujących możliwość wymiany pirackich treści. Więcej na temat P2P na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Peer-to-peer.

widzenia wartości naukowej pracy, ale przede wszystkim pozwala spojrzeć na zjawisko cyberprzestępczości w ujęciu dynamicznym, z perspektywy poziomów funkcjonowania cyberprzestrzeni. Popularne w literaturze grupowanie cyberprzestępstw z zastosowaniem kryterium dobra prawnie chronionego będącego przedmiotem zamachu - choć niesie ze sobą niewątpliwe korzyści porządkujące, stanowi w ocenie Autora niniejszej pracy rozwiązanie coraz bardziej nieefektywne w stosunku do nowoczesnej cyberprzestępczości, powodując konieczność wielokrotnego kwalifikowania tego samego czynu do kolejnych wyróżnianych kategorii. Nieścisłość ta powodowana jest odwołaniem do kryterium dóbr chronionych, które nie zapewnia już należytego poziomu rozłączności wydzielanych zbiorów. Przykładowo, przestępstwo *hackingu* może *de facto* zostać popełnione tak przeciwko ochronie informacji (w tym ich poufności, integralności lub dostępności), jak również wiarygodności dokumentów, czy też bezpieczeństwu państwa - w zależności od szczegółowego opisu działania sprawcy, a także funkcjonalności atakowanego systemu teleinformatycznego. Co więcej, pojedyncze przestępstwo może także naruszać określoną kombinację dóbr prawnie chronionych (np. nieuprawniona zmiana treści dokumentu z konieczności logicznej wiąże się z wcześniejszym naruszeniem jego poufności). Zaprezentowany wyżej autorski podział cyberprzestępczości wydaje się opierać tej słabości, choć należy sądzić, że kolejne lata przyniosą nowe formy cyberprzestępstw, wymagające prowadzenia dalszych analiz.

Podobnie jak w przypadku poprzednich części pracy, także i tym razem jednym z założeń konstrukcyjnych całości rozdziału stało się podjęcie próby uporządkowania siatki pojęciowej stosowanej w obszarze *cyberbezpieczeństwa*, która z uwagi na wzajemne przenikanie się oraz uzupełnianie poszczególnych metod popełniania cyberprzestępstw - nie zawsze dostarcza odpowiednio precyzyjnych narzędzi. Warto także od razu dodać, że wiele ze stosowanych w rozdziale określeń należy do żargonu informatycznego, w którym językiem dominującym jest oczywiście język angielski.

Dla potrzeb sformułowania wniosków, jak i szeregu postulatów *de lege lata,* jak i *de lege ferenda* całość rozważań zakończona została analitycznym zestawieniem cech poszczególnych przestępstw, uwidaczniającym właściwości całego zjawiska cyberprzestępczości.

Pierwsza z wydzielonych kategorii cyberprzestępstw obejmuje czyny występujące w zakresie transmisji danych, rozumianej jako całokształt procesu przesyłania danych pomiędzy systemami teleinformatycznymi za pośrednictwem łączącej ich sieci (*vide* uwagi zawarte w rozdziale III). Kategoria ta obejmuje zarówno czyny skierowane przeciwko bezpieczeństwu transmisji danych, jak i czyny naruszające przyjęte zasady obsługi ruchu

w sieci. Przedstawione połączenie wynika z faktu, że sama transmisja może stanowić tak przedmiot przestępstwa, jak również szczególne narzędzie do jego popełnienia. Do tak zakreślonej kategorii cyberprzestępstw w zakresie transmisji danych, w szczególności zaliczyć należy bezprawne:

1) podsłuchiwanie treści transmisji;
2) modyfikowanie lub zakłócanie treści transmisji; oraz,
3) zalewanie systemów nadmierną transmisją.

Poszczególne cyberprzestępstwa w zakresie transmisji danych - wraz z odnośnymi metodami ataku, zaprezentowane zostały z zachowaniem powyższej kolejności.

Na wstępie do niniejszego rozdziału konieczne jest także dokonanie istotnej uwagi językowej odnoszącej się do stosowanego tłumaczenia własnego postanowień Konwencji Rady Europy o cyberprzestępczości. Jak było podkreślane w rozdziale 4. pracy, z uwagi na komparatystyczny charakter przywołań przedmiotowego aktu międzynarodowego, ale także fakt, iż oficjalnie wykonane tłumaczenie konwencji w ocenie Autora niniejszej pracy istotnie odbiega od jej tłumaczenia językowego, wręcz do stopnia, w którym zniekształcona jest rzeczywista treść Konwencji - na potrzeby analizy tegoż dokumentu stosowane jest tłumaczenie własne, wykonane przy najwyższej staranności o zachowanie odpowiedniości wyrażeń o konotacji technicznej. Nieco na marginesie należy również podkreślić, iż oficjalna ratyfikacja Konwencji została dokonana przez Polskę przeszło 10 lat po wprowadzeniu do Kodeksu karnego zmian mających na celu faktyczną implementację jej zapisów, a zatem implementacja nie była wykonywana w oparciu o tłumaczenie opublikowane później w Dzienniku Ustaw. Nieco ironicznie, można powiedzieć, iż w przypadku tłumaczenia Konwencji o cyberprzestępczości dokonana została indukcja zwrotna - w której tłumaczenie dokumentu zostało sporządzone w oparciu o już dokonany sposób implementacji postanowień normatywnych. Dla zachowania rzetelności wywodu, obok stosowanego tłumaczenia własnego, w rozdziale zamieszczone są także - porównawczo, zwroty pochodzące z Konwencji w oficjalnym przekładzie na język polski.

1. Podsłuchiwanie treści transmisji

Podsłuchiwanie treści transmisji to cyberprzestępstwo skierowane przeciwko poufności informacji[4]. Przestępstwo to polega na uzyskaniu w dowolny sposób bezprawnego dostępu do danych oraz informacji, które przekazywane są w cyberprzestrzeni pomiędzy

[4] A. Adamski, Prawo karne komputerowe, CH Beck, Warszawa 2000, s. 55.

systemami - stronami zachodzącej komunikacji. Należy zauważyć, że komunikacja w cyberprzestrzeni możliwa jest nie tylko pomiędzy dwoma użytkownikami (ludźmi), ale także użytkownikiem, a systemem (np. przy logowaniu się do usługi bankowości elektronicznej), a nawet pomiędzy dwoma systemami (np. w sytuacji automatycznej aktualizacji oprogramowania). Specjalistyczne oprogramowanie wykorzystywane do przechwytywania danych określane jest często mianem *spyware*[5].

Analizując przedmiot zamachu przestępstwa podsłuchiwania transmisji, podkreślenia wymaga stwierdzenie, że dla wystąpienia bezprawnego podsłuchu transmisji nie jest istotne, czy przesyłane w sieci dane (analizowana typizacja nie obejmuje innych form przekazu[6]) zostały uprzednio zabezpieczone w szczególny sposób, np. zaszyfrowane, bowiem podsłuch narusza powszechne w demokratycznych systemach prawnych prawo tajemnicy komunikacyjnej, zwanej też tajemnicą korespondencji. Prawo to chronione jest zarówno przepisami krajowymi - najczęściej już na poziomie konstytucyjnym, jak również przez stosowne umowy międzynarodowe, w szczególności zaś Międzynarodowy Pakt Praw Obywatelskich i Politycznych z 1966 r. oraz Europejską Konwencję o Ochronie Praw Człowieka i Podstawowych Wolności z 1950 r.[7]. W dokumentach tych zawarte zostały odpowiednio przepisy gwarantujące ochronę korespondencji przed bezprawną ingerencją (art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych[8]), a także poszanowanie korespondencji (art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[9]). W polskim systemie prawnym tajemnicę komunikacji gwarantuje przede wszystkim Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., jak również przepisy działu VII ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne[10], który to dział zatytułowany został: „Tajemnica telekomunikacyjna oraz ochrona danych użytkowników końcowych". Pogłębione rozważania odnoszące się do przepisów krajowych prezentowane są w dalszej części niniejszej pracy.

Od strony technicznej, do podsłuchiwania transmisji danych wykorzystywany jest szereg zróżnicowanych ataków. W stosunku do transmisji przewodowej możliwe jest w szczególności podsłuchiwanie ruchu sieciowego na jednym z węzłów pośredniczących w wymianie danych, jak również odpowiednie przekierowanie ruchu tak, aby ruch ten

---

5 M. Siwicki, Cyberprzestępczość, C. H. Beck, Warszawa 2013, s. 122.
6 *Ibidem*, s. 125.
7 Wskazuję za: A. Adamski, Prawo karne komputerowe, CH Beck, Warszawa 2000, s. 55 i 56.
8 Tekst opublikowany w Dz. U. z 1977 Nr 38, poz. 167.
9 Pełny tekst Konwencji w języku polskim dostępny jest na stronie internetowej pod adresem: http://www.echr.coe.int/NR/rdonlyres/7B5C268E-CEB3-49A5-865F-06286BDB0941/0/POL_CONV.pdf.
10 Dz. U. z 2004 Nr 171, poz. 1800, z późn. zm.

podążał za pośrednictwem systemu kontrolowanego przez atakującego. W stosunku do transmisji bezprzewodowej (np. w popularnej obecnie technologii radiowej Wi-Fi[11]), możliwe jest także przechwytywanie pakietów danych rozgłaszanych w postaci fal radiowych w eterze. Ataki polegające na przechwytywaniu danych jeszcze niewysłanych z komputera, np. stosowanie tzw. *keyloggerów*, czyli rozwiązań programowych lub programowo-sprzętowych, śledzących ciągi znaków wpisywanych z klawiatury, przybliżone zostały w części 4. rozdziału. Ataki te, choć również służą do przechwytywania danych przetwarzanych w systemach teleinformatycznych, nie są atakami występującymi na etapie transmisji danych w sieci.

Zgodnie z tym co zostało powiedziane w rozdziale III pracy, dane przesyłane pomiędzy systemami pokonują w cyberprzestrzeni skomplikowaną drogę, przeskakując pomiędzy kolejnymi węzłami pośredniczącymi, znajdującymi się pomiędzy nadawcą, a odbiorcą danych. Dokładna cyber-ścieżka łącząca komputer użytkownika znajdującego się np. w Polsce, z serwerem zlokalizowanym w USA, ustalana jest w procesie tzw. trasowania ruchu. Nierzadko nawiązanie połączenia pomiędzy dwoma, geograficznie oddalonymi od siebie systemami wymaga wykonania nawet kilkunastu skoków - co pociąga za sobą udział kilkunastu węzłów pośredniczących. Węzły te - jak każdy element cyberprzestrzeni oraz podbudowującej ją infrastruktury, mogą zostać skutecznie zaatakowane w sposób zapewniający atakującemu dostęp do przesyłanych przez nie danych. Z uwagi na fakt, iż ruch sieciowy w ogromnej mierze obsługiwany jest przez duże podmioty profesjonalne - to jest dostawców usług sieciowych lub operatorów telekomunikacyjnych, przełamanie zabezpieczeń chroniących zastosowane rozwiązania infrastrukturalne z pewnością nie należy do rzeczy łatwych, mogąc nawet wymagać dostępu do informacji wewnętrznych danego usługodawcy. W przypadku skutecznego ataku możliwe jest jednak częściowe przejęcie kontroli nad danym węzłem, umożliwiające przechwytywanie wędrujących za jego pośrednictwem pakietów danych. Ataki skutkujące przejęciem kontroli nad systemem teleinformatycznym przybliżone zostaną w części 4. rozdziału, choć stanowią w tym wypadku element przygotowania podsłuchu.

Zupełnie inna filozofia ataku przyświeca natomiast drugiej z wyżej wymienionych metod podsłuchiwania transmisji danych, polegającej na odpowiednim przekierowaniu ruchu sieciowego, tak aby ruch ten podążał bezpośrednio do systemu, który kontrolowany jest przez osobę atakującą. Bezpośrednim przedmiotem ataku są w tym przypadku mechanizmy

[11] Z ang. *Wireless Fidelity*. Więcej na temat technologii Wi-Fi oraz jej certyfikacji znaleźć można na stronie internetowej pod adresem: http://www.wi-fi.org/.

trasowania ruchu. Dla ukrycia incydentu, podsłuchana transmisja jest przekazywana dalej, tak by dotarła do swojego prawowitego adresata nie budząc podejrzeń, jakie wiązałyby się z jej zaginięciem w sieci. Dla skuteczności ataku niezbędne jest bowiem ażeby systemy biorące udział w podsłuchiwanej transmisji były przekonane, że komunikacja zachodzi wyłącznie pomiędzy uprawnionymi użytkownikami. Ewentualna transmisja zwrotna ponownie przechodzi ścieżkę wiodącą przez system prowadzący atak, zapewniając pełną kontrolę wzajemnie komunikowanych treści. W pewnym uproszczeniu, metoda ta polega na spreparowaniu dodatkowego węzła pośredniczącego oraz wprowadzeniu go w łańcuch transmisji danych, z czym koresponduje angielska nazwa wskazanego ataku: *man-in-the-middle* (człowiek-pośrodku)[12].

Jedną z podstawowych metod przeprowadzenia ataku typu *man-in-the-middle* jest tzw. *IP spoofing*, polegający na wysyłaniu pakietów danych opatrzonych zmodyfikowanymi adresami IP, służącymi do identyfikacji nadawcy oraz odbiorcy danych w cyberprzestrzeni. Wskazana technika może zostać wykorzystana zarówno w celu ukrycia rzeczywistego źródła ruchu sieciowego (np. dla ukrycia tożsamości osoby przeprowadzającej atak), jak też do przechwycenia transmisji kierowanej do innego użytkownika w przypadku podszycia się pod cudzy adres IP[13]. Poprzez wysyłanie odpowiednio spreparowanych pakietów danych możliwe jest takie ukształtowanie ścieżki komunikacji zachodzącej *teoretycznie* pomiędzy dwoma systemami, aby każdy z tych systemów *de facto* wysyłał informacje do komputera atakującego, pozostając jednak w przekonaniu, że transmisja danych dociera wyłącznie do uprawnionego odbiorcy. Jedną z podstawowych metod zapobiegania atakom tego typu jest wprowadzenie zasad wzajemnego uwierzytelniania się stron komunikacji, w szczególności z zastosowaniem rozwiązań kryptograficznych.

Inną metodą bezprawnego przekierowywania transmisji danych, jest tzw. zatruwanie tablic DNS[14], noszące w oryginale nazwę *DNS cache poisoning* lub też *DNS spoofing*[15]. Nawiązując do rozważań zawartych w rozdziale III, DNS - czyli *Domain Name System,* to w uproszczeniu usługa pozwalająca na automatyczne przekształcanie łatwych do

---

[12] Przykładowy atak typu *man-in-the-middle* opisany został w publikacji „*Common Control System Vulnerability*" - w tłumaczeniu: „Powszechne podatności systemów kontroli" (tłumaczenie własne), przygotowanej przez amerykański zespół CERT. US CERT stanowi część Departamentu Bezpieczeństwa Krajowego USA (*Department of Homeland Security*). Tekst opracowania dostępny jest na stronie internetowej pod adresem: http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf.

[13] A. Farha, *IP Spoofing*, *The Internet Protocol Journal*, *Volume* 10, *No.* 4, 2007. Opracowanie przygotowane dla CISCO. Pełen tekst publikacji dostępny jest na stronie internetowej pod adresem: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html

[14] Na metody związane z zatruwaniem DNS uwagę zwraca także J. Kosiński w: Regulacje karnoprawne w dziedzinie zwalczania zagrożeń w sieci, Przegląd policyjny Nr 2 (90)/2008, Szczytno 2008, s. 95.

[15] Nazwy te używane są zamiennie, tak np. http://en.wikipedia.org/wiki/DNS_spoofing.

zapamiętania adresów stron WWW (tzw. nazw mnemonicznych, np. www.uw.edu.pl) na ich aktualne adresy IP, stanowiące zrozumiałe dla komputerów identyfikatory stron w sieciach rozległych oraz sieciach lokalnych. Przykładowo, po wykonaniu komendy *ping* wobec przytoczonego w przykładzie adresu: www.uw.edu.pl, adres ten w chwili badania zgłasza się pod numerem IP: 193.0.113.10. Zatrucie DNS sprowadza się w efekcie do takiego przerobienia zapisów DNS, aby wykonywana transmisja kierowana była w sposób automatyczny do *niewłaściwego* adresu IP, identyfikującego zakończenie sieci, do którego podłączony jest system atakujący. Zatrucie DNS może zostać dokonane zarówno poprzez odpowiednie zniekształcenie tablic dostarczanych przez dostawców usług sieciowych lub tablic przetwarzanych lokalnie na komputerze ofiary, jak również poprzez włączenie się do transmisji danych i udzielenie mylnej odpowiedzi DNS na pytanie zadane przez system ofiary[16]. Serwery DNS zawierające fałszywe informacje o adresach nazywa się „zatrutymi". Powyższe działania mogą być wykonywane przez cyberprzestępcę zarówno „*samodzielnie*", jak również z zastosowaniem odpowiednio przygotowanego w tym celu oprogramowania – w tym wirusów komputerowych oraz specjalnych skryptów, zdolnych nawet do automatycznego wyszukiwania ofiar ataków.

W związku z wciąż rosnącą popularnością technologii bezprzewodowych, w szczególności wykorzystujących technologię Wi-Fi, istotnym obszarem podsłuchiwania danych staje się aktualnie także łączność radiowa. W przypadku korzystania z tzw. *hot-spotów* (czyli punktów bezprzewodowego dostępu do Internetu, zlokalizowanych np. w kawiarniach), czy posługiwania się routerem wykorzystującym technologie radiowe do wygodnego, bezprzewodowego dostarczania sieci do komputera, wykonywana transmisja rozgłaszana jest w eterze w postaci fal radiowych, które nie podążają wyłącznie na linii komputer - router, lecz najczęściej rozsiewane są dookólnie, nierzadko w zasięgu nawet stu metrów. Fale te nie tylko poddają się możliwości łapania przy zastosowaniu odbiorników wbudowanych w urządzenia bezprzewodowe, ale także umożliwiają prowadzenie analizy ruchu sieciowego. Stąd też, w przypadku technologii bezprzewodowych tak istotna staje się kwestia ochrony kryptograficznej transmisji przy zastosowaniu odpowiednio silnego hasła, uniemożliwiającego lub przynajmniej powodującego istotne utrudnienia w odczytaniu treści wymienianych informacji. Zaszyfrowane pakiety danych można oczywiście tak samo łatwo przechwycić w czasie rozgłaszania w eterze, jednak ich treść pozostaje nieznana aż do momentu odszyfrowania wiadomości. Warto nadmienić, że starsze zabezpieczenia,

[16] O metodach tych można przeczytać więcej na stronie internetowej pod adresem: http://dnscurve.org/forgery.html.

jak np. WEP, nie stanowią dziś żadnej bariery ochronnej, z łatwością poddając się nowoczesnym metodom analizy[17]. Podsłuchiwanie transmisji bezprzewodowych możliwe jest także na wskutek przejęcia kontroli nad urządzeniami sieciowymi, np. domowym routerem obsługującym bezprzewodową sieć lokalną. Ponieważ cały ruch użytkowników sieci kierowany jest w tym przypadku za pośrednictwem routera, złamanie jego wewnętrznych zabezpieczeń powoduje możliwość inwigilacji transmitowanych danych. Producenci tego typu urządzeń wielokrotnie podkreślają m. in. konieczność zmiany domyślnego hasła administratora, zapewniającego pełen dostęp do ustawień routera.

Analizując przestępstwa przeciwko transmisji danych występujących w kontekście sieci bezprzewodowych, warto także dodać, że fakt przejęcia kontroli nad siecią bezprzewodową może również zostać wykorzystany do przeprowadzenia dalszego ataku z pozycji przejętej sieci. Działanie takie pozwala nie tylko na ukrycie tożsamości prawdziwego sprawcy, ale jednocześnie ściąga zainteresowanie organów wymiaru sprawiedliwości na osobę postronną, której jedyna *wina* polega na nienależytym zabezpieczeniu posiadanego punktu dostępowego do Internetu[18].

W jaki sposób zatem penalizowane jest przestępstwo bezprawnego podsłuchiwania transmisji danych? Za punkt wyjścia do rozważań o charakterze prawniczym przyjąć można postanowienia wielokrotnie już przywoływanej w pracy Konwencji Rady Europy o cyberprzestępczości[19], której przepisy stanowią podstawę dla regulacji karnych omalże czterdziestu państw z całego świata. Na gruncie Konwencji, bezprawne podsłuchiwanie transmisji danych, nazywane w dokumencie „*Illegal interception*" - a więc „bezprawnym przechwytywaniem" (w tłumaczeniu oficjalnym „Nielegalne przechwytywanie danych"[20]), opisane zostało w art. 3, stanowiącym, że:

> „Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego, popełnionego umyślnie czynu polegającego na bezprawnym przechwytywaniu danych komputerowych przekazywanych do, z lub wewnątrz systemu komputerowego

---

[17] Zgodnie z doniesieniami prasowymi, złamanie sieci zabezpieczonej przy zastosowaniu technologii WEP już w 2005 r. zajmowało jedynie 3 minuty przy użyciu zwykłego komputera z zainstalowanym ogólnodostępnym oprogramowaniem. Źródło: http://www.smallnetbuilder.com/index.php?option=com_content&task=view&id=24251&Itemid=100.

[18] Wskazana działalność określana jest w języku technicznym mianem *war driving*. Więcej na ten temat na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Wardriving.

[19] Tytuł oryginalny: *Convention on Cybercrime*, CETS Nr: 185. Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[20] Tłumaczenie oficjalne zawarte w tekście Konwencji podanym do powszechnej wiadomości Przez Prezydenta RP w dniu 27 maja 2015 r., Dz. U. z 2015 r. poz. 728.

w ramach transmisji o nie-publicznym charakterze, dokonywanym przy użyciu środków technicznych, w tym przechwytywanie ulotu elektromagnetycznego systemu komputerowego, zawierającego takie dane komputerowe. Strona może wprowadzić dodatkowe wymogi popełnienia przestępstwa z nieuczciwym zamiarem lub w stosunku do systemu komputerowego, który połączony jest z innym systemem komputerowym."[21].

Uzupełniając treść przepisu na potrzeby prowadzenia jego dalszej analizy, „dane komputerowe" - o czym pisano już w poprzednim rozdziale pracy, zdefiniowane zostały na gruncie Konwencji Budapesztańskiej, jako „wszelka reprezentacja faktów, informacji lub koncepcji w formie odpowiedniej do przetwarzania w systemie komputerowym, w tym także oprogramowanie zdolne wykonywać określone funkcje". Poszerzając wcześniejsze rozważania, warto dodać, że zgodnie z Raportem Wyjaśniającym do Konwencji[22] - stanowiącym istotne źródło informacji uzupełniających postanowienia komentowanej konwencji, przytoczona definicja oparta została na rozwiązaniach pochodzących z norm Międzynarodowej Organizacji Standaryzacyjnej (ISO). Wyraźne wskazanie na „formę odpowiednią do przetwarzania w systemie" miało na celu jednoznaczne określenie, że danymi komputerowymi, są dane, które komputer może przetwarzać bez konieczności poddawania ich żadnym dodatkowym, wcześniejszym przekształceniom (dane zrozumiałe dla komputera). W efekcie, danymi komputerowymi w szczególności nazwane zostały dane występujące w postaci elektronicznej, zapisywane na stosownych nośnikach danych (np. na dysku twardym, czy płycie CD, DVD, czy BD) lub przetwarzane w pamięci operacyjnej komputera (RAM). Dla uznania danych za „dane komputerowe" nie ma przy tym znaczenia ich treść - zaś ważna jest jedynie forma. Zawarte w definicji postanowienie, że przez „dane komputerowe" należy rozumieć także oprogramowanie, wydaje się w tej sytuacji nadmiarowe.

Zgodnie z przyjętą systematyką aktu, przechwytywanie danych zaliczone zostało do kategorii przestępstw przeciwko poufności, integralności oraz dostępności danych i systemów

---

[21] Art. 3 Konwencji o cyberprzestępczości. W oryginale: „*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*". Tłumaczenie własne. W oficjalnym przekładzie zamiast „danych komputerowych" oraz „systemu komputerowego" stosowane są odpowiednio „dane informatyczne" oraz „systemy informatyczne".

[22] *Explanatory Report*, pełen tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

komputerowych (tytuł 1. sekcji 1. rozdziału II.). Uzupełniająco, w Raporcie Wyjaśniającym do Konwencji, przeczytać można o art. 3, że „Celem przepisu jest ochrona prawa do prywatności komunikacji danych”[23].

Analizując przytoczony przepis art. 3 stwierdzić można, że dla ukonstytuowania stypizowanego w nim przestępstwa przechwytywania danych, niezbędne jest jednoczesne spełnienie następujących przesłanek:

- wystąpienie dowolnej transmisji danych komputerowych, zachodzącej w którymkolwiek kierunku, tak pomiędzy dwoma systemami, jak również wewnątrz pojedynczego systemu (np. pomiędzy procesorem, a kartą graficzną i monitorem). Przesłanka ta może zostać ograniczona przez państwo-stronę Konwencji do ruchu pomiędzy dwoma systemami,
- zachowanie nie-publicznego charakteru wykonywanej transmisji, oraz
- zastosowanie środków technicznych w celu umyślnego oraz bezprawnego przechwytywania danych wymienianych w ramach tak scharakteryzowanej transmisji, również poprzez przechwytywanie ulotu elektromagnetycznego urządzenia (o tym, czym jest ulot pisano w rozdziale III.).

Odnośnie przesłanki pierwszej, zauważyć należy, że Konwencja w sposób wyraźny przewidziała możliwość wykonywania transmisji danych w ramach jednego systemu komputerowego, w domyśle dzieląc taki system na szereg wzajemnie komunikujących się podzespołów. Przyjęte rozwiązanie umożliwiło w efekcie objęcie regulacją karną nie tylko przechwytywanie danych wytransmitowanych już poza system (danych „wędrujących w sieci”), ale także przechwytywanie danych przetwarzanych wyłącznie lokalnie - to jest wewnątrz systemu. Przechwytywanie danych w drugim z wymienionych wypadków dokonywane jest w cyberprzestrzeni w szczególności za pomocą specjalistycznych narzędzi szpiegujących (najczęściej programowych), które po potajemnym zainstalowaniu w systemie ofiary, rozpoczynają zbieranie określonych kategorii informacji oraz wysyłają je za pośrednictwem sieci do atakującego. Zainfekowany komputer staje się w efekcie samodzielnym narzędziem podsłuchowym skierowanym przeciwko swojemu uprawnionemu użytkownikowi, potajemnie przekazując dalej dane, które nie miały w ogóle opuścić systemu. Zgodnie z przyjętym na gruncie pracy podziałem cyberprzestępczości, ataki polegające na wprowadzaniu bezprawnych zmian w systemie (np. instalowanie oprogramowania

[23] Pkt 51 Raportu Wyjaśniającego. W oryginale: „*This provision aims to protect the right of privacy of data communication.*”. Tłumaczenie własne.

szpiegującego), w tym skierowane przeciwko danym przetwarzanym lokalnie, przybliżone będą szeroko w części 4. rozdziału. Szczególnym przypadkiem przechwytywania danych przetwarzanych lokalnie, który w sposób wyraźny objęty został regulacją Konwencji, jest natomiast analiza ulotu elektromagnetycznego, pozwalająca na zbierania informacji pochodzących z systemu, który może pozostawać nawet w pełnej separacji od środowiska sieciowego - innymi słowy, być w ogóle wyłączonym z cyberprzestrzeni.

Dla oceny wystąpienia przesłanki drugiej, to jest nie-publicznego charakteru transmisji, niezbędne wydaje się przeprowadzenie analizy, czy podsłuchiwana transmisja miała być udostępniona nieokreślonemu kręgowi odbiorców, czy też zawężona podmiotowo wyłącznie do ściśle określonych adresatów, pragnących komunikować się z zachowaniem poufności. Zgodnie z Raportem Wyjaśniającym do Konwencji,

> „Wyrażenie „nie-publiczna" określa charakter samej transmisji (komunikacji) nie zaś charakter danych, które są transmitowane. Wymieniane dane mogą stanowić powszechnie dostępne informacje, co nie zmienia faktu, że strony mogą życzyć sobie komunikować się z zachowaniem poufności. [...] Tym samym, wyrażenie „nie-publiczne" nie wyklucza ochrony komunikacji dokonywanych za pośrednictwem publicznych sieci." [24].

O ile zatem strony komunikacji wykorzystują przyjęte środki programowe lub techniczne w sposób zakładający poufność wymiany danych, o tyle transmisja taka staje się transmisją nie-publiczną. Zgodnie z brzmieniem przepisu, nie ma przy tym znaczenia fakt, czy komunikowane dane zostały w jakikolwiek sposób uprzednio zabezpieczone, np. zaszyfrowane, zaś istotne jest, że strony chciały, aby treść komunikatu pozostała dostępną wyłącznie dla nich. Błędne wykorzystanie aplikacji, powodujące upublicznienie przekazywanych materiałów wbrew intencji stron, nie może być zatem poddawane subsumcji karnej.

W zakresie przesłanki trzeciej, Konwencja stanowi, że przechwytywanie danych może być popełnione jedynie umyślnie oraz pod warunkiem, że jest bezprawne. Granicę bezprawności wyznacza przede wszystkim zgoda użytkownika systemu, który może świadomie zezwolić zainstalowanemu w swoim systemie oprogramowaniu na zbieranie określonych danych, np. w celach analitycznych, reklamowych, czy dla poprawy jakości świadczonych usług (to ostatnie rozwiązanie znane jest przede wszystkim z samych systemów

---

[24] Pkt 54 Raportu Wyjaśniającego. W oryginale: „*The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. [...] Therefore, the term 'non-public' does not per se exclude communications via public networks.*". Tłumaczenie własne.

operacyjnych). Określając granicę bezprawności niezbędne staje się także uwzględnienie panujących w sieci zwyczajów lub praktyk, zezwalających np. na stosowanie tzw. plików *cookie*[25], służących do zdalnego zapisywania na komputerze użytkownika informacji na temat jego sieciowej aktywności (np. faktu zalogowania się oraz wylogowania ze strony danego sklepu internetowego)[26]. Zgodnie z art. 3 Konwencji, przechwytywanie danych wykonywane jest przy zastosowaniu środków technicznych, które to pojęcie należy rozumieć szeroko, jako obejmujące wszelkiego rodzaju urządzenia, narzędzia, czy programy, które mogą być stosowane tak bezpośrednio w stosunku do atakowanego systemu, jak również zakładane na łączach, czy wykorzystywane do gromadzenia danych przesyłanych w ramach transmisji bezprzewodowej. Zgodnie z Raportem Wyjaśniającym, wymóg stosowania środków technicznych miał w pierwszej kolejności zapobiec nadmiernej kryminalizacji bliżej nieokreślonych kategorii czynów[27].

Dokonując analizy prawnej przestępstwa podsłuchiwania transmisji danych na gruncie regulacji krajowych, w pierwszej kolejności należy odnieść się do przedmiotu ochrony prawnej, który potencjalnie może zostać naruszony takim czynem. Zgodnie z art. 49 Konstytucji:

„Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.”

Stosowne ograniczenia prawa tajemnicy komunikacyjnej wynikają między innymi z regulacji określających zasady działania wymiaru sprawiedliwości - w tym uprawnienia do prowadzenia kontroli operacyjnej.

Zgodnie zaś z art. 159 ustawy - Prawo telekomunikacyjne, tajemnica komunikacyjna obejmuje:

„1) dane dotyczące użytkownika;
2) treść indywidualnych komunikatów;
3) dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;

---

25 Więcej na temat tzw. ciasteczek na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Ciasteczko.
26 Na dopuszczalność tego typu praktyk wskazuje wprost Raport Wyjaśniający do Konwencji w pkt 58.
27 Raport Wyjaśniający, pkt 53.

4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;
5) dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń."

W świetle przytoczonej regulacji art. 159 ustawy - Prawo telekomunikacyjne, zasadne wydaje się przyjęcie założenia, że na gruncie polskiego prawa bezprawne podsłuchiwanie transmisji może w efekcie dotykać potencjalnie nie tylko danych komunikowanych, ale także np. danych o samym fakcie zestawienia połączenia, czy danych lokalizujących mobilne urządzenia sieciowe (w dzisiejszych czasach właściwie każdy telefon komórkowy posiada funkcjonalności sieciowe umożliwiając odwiedzanie stron WWW, czy przynajmniej obsługę poczty elektronicznej). Na marginesie, warto w tym miejscu dodać, że zbieranie danych na temat ruchu sieciowego użytkowników stanowi obecnie intratne zajęcie, pozwalając na prowadzenie szeroko zakrojonych analiz rynkowych oraz kierowanie personalizowanych reklam. Dla przykładu - nie jest dziś niczym nadzwyczajnym by na amerykańskiej stronie internetowej znaleźć reklamę polskiej firmy, której witrynę WWW odwiedziło się kilka dni wcześniej.

Obowiązująca w Polsce regulacja karna penalizująca podsłuchiwanie (czy też przechwytywanie) transmisji danych, wprowadzona została do Kodeksu karnego, znajdując miejsce w przepisach rozdziału XXXIII, zatytułowanego „Przestępstwa przeciwko ochronie informacji". Przyjęta regulacja oparta została na przeanalizowanych wyżej rozwiązaniach Konwencji o cyberprzestępczości (które dla uniknięcia powtórzeń prezentowane będą dalej jedynie sygnalizacyjnie) oraz z uwzględnieniem przepisów Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[28] - należy jednak podkreślić, że wskazana decyzja nie wprowadziła karalności samego podsłuchu transmisji, typizując inne rodzaje cyberprzestępstw, które ujęte zostały wspólnie w przepisie krajowym.

Znamiona przestępstwa podsłuchiwania transmisji danych wprowadzone zostały w Kodeksie karnym do art. 267 § 1 i 3 oraz art. 269b § 1. Po wejściu w życie nowelizacji

[28] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW. Pełny tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:PL:PDF.

z października 2008 r.[29], przepisy te przyjęły następujące brzmienie:

„Art. 267 § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.", oraz

„Art. 269b § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.".

Zawężając analizę wskazanych przepisów do oceny prawnej przechwytywania danych w cyberprzestrzeni, w pierwszej kolejności należy zauważyć, że na gruncie polskiego prawa krajowego, odrębnej penalizacji poddane zostały czyny polegające na bezprawnym[30]:

- zakładaniu lub posługiwaniu się oprogramowaniem służącym do uzyskiwania informacji (art. 267 § 3),
- wytwarzaniu, pozyskiwaniu lub udostępnianiu takiego oprogramowania (art. 269b § 1),
- uzyskiwaniu dostępu do informacji poprzez podłączenie się do sieci telekomunikacyjnej lub przełamanie bądź też ominięcie jakiegokolwiek zabezpieczenia chroniącego daną informację (art. 267 § 1), oraz
- pozyskiwaniu haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanej w systemie komputerowym - jako szczególny rodzaj podsłuchu (art. 269b § 1).

Jako przedmiot przestępstwa wskazane zostały w powyższych przypadkach:

---

[29] Dz. U. Nr 214, poz. 1344.

[30] A. Lach, Kodeks karny. Komentarz, WK, 2016, system LEX - komentarz do art. 267 k.k. oraz W. Wróbel, Kodeks karny, Część szczególna. Tom II. Komentarz do art. 117-277 k.k., pod red. A. Zolla, A. Barczak-Oplustil, M. Bielski, G. Bogdan, Z. Ćwiąkalski, M. Dąbrowska-Kardas, J. Majewski, J. Raglewski, M. Szewczyk, M. Wróbel, LEX 2013, system LEX - komentarz do art. 267, 269b k.k.

1) informacje - które zastąpiły znane z Konwencji o cyberprzestępczości „dane komputerowe"; oraz,
2) hasła komputerowe, kody dostępu i inne, podobne *treści* - ujęte w przepisie w zbiorczą kategorię „danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej".

W kontekście powyższego wyliczenia, zauważyć można, że na gruncie analizowanych przepisów „informacjami" nazwane zostały w rezultacie zasoby komputerowe, które przetwarzane są bądź to lokalnie, bądź też transmitowane za pośrednictwem sieci telekomunikacyjnych, zaś „danymi umożliwiającymi dostęp" - swojego rodzaju *klucze*, umożliwiające zapoznanie się z informacjami. W świetle terminologii przyjętej w Konwencji o cyberprzestępczości oraz Decyzji Ramowej Rady w sprawie ataków na systemy informatyczne, jak również znaczeń tych wyrazów przyjętych na gruncie języka technicznego, należy ocenić, że rozwiązanie to nie zapewnia należytego poziomu przejrzystości legislacji, w istocie mieszając kategorie „danych" i „informacji", jednocześnie nie rozstrzygając statusu oprogramowania (czy jest informacją?). Uzupełniająco, na gruncie Decyzji UE, „dane komputerowe" zdefiniowane zostały - analogicznie do rozwiązań przyjętych wcześniej w Konwencji (przeanalizowanych wyżej), jako:

> „wszelkie przedstawienie faktów, informacji lub koncepcji w formie odpowiedniej do przetwarzania w systemie informatycznym, włącznie z programem odpowiednim do spowodowania wykonania funkcji przez system"[31].

Na tle powyższych rozważań rodzą się istotne wątpliwości, czy podsłuchanie:

- fragmentu transmisji - a w efekcie przechwycenie jedynie części pliku (określonej ilości *danych*), która to część sama w sobie nie wystarczy do odczytania *informacji*[32],
- transmisji zaszyfrowanej, nie zawierającej *informacji* gotowej do odczytania, lub też,
- transmisji, w ramach której przesyłany jest wykonywalny kod programu komputerowego,

winno być kwalifikowane na gruncie polskiej ustawy karnej, jako przestępstwo? Brak desygnatu pojęcia „informacja", przekreśla bowiem możliwość wystąpienia ustawowej przesłanki „dostępu do informacji", czy też „uzyskania informacji" wykluczając tym samym byt samego przestępstwa uregulowanego w art. 267 § 1 oraz § 3 Kodeksu karnego. Wskazana

---

[31] Art. 1 lit. b Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW.

[32] W. Wróbel, op. cit., system LEX - komentarz do art. 267 k.k.

wątpliwość znajduje swoje istotne odzwierciedlenie technologiczne. W odniesieniu do kwestii przechwycenia fragmentu transmisji, w cyberprzestrzeni możliwe jest podsłuchiwanie transmisji danych „po kawałku”, w drodze przechwytywania poszczególnych fragmentów transmisji wędrującej poprzez kolejne węzły, w taki sposób aby całość informacji wynikała dopiero z odpowiedniego zestawienia przejętych porcji danych. Na marginesie, warto wskazać, że od strony technicznej możliwe jest również rozmyślne udostępnianie posiadanych zasobów komputerowych w częściach, nie zaś w całości, celem uniknięcia zarzutu rozpowszechniania określonych treści. Na wskazanej zasadzie oparta została między innymi technologia *torrent*[33], w praktyce wykorzystywana głównie do propagowania treści naruszających prawa autorskie. W technologii tej, poszczególni użytkownicy sieci *torrent* pobierają od siebie jedynie fragmenty plików poddanych ochronie prawno autorskiej (najczęściej filmów), w taki jednak sposób, aby pod koniec wymiany każdy z użytkowników dysponował całością każdego pliku. Rozwiązanie to powoduje, że żadnego z poszczególnych użytkowników sieci nie można oskarżyć o wytransmitowanie całości zasobu, który dopiero po spojeniu tworzy plik komputerowy nadający się do odtworzenia (połowa pliku nie równa się bowiem np. pierwszej godzinie filmu). Przechodząc do kwestii przechwytywania transmisji szyfrowanych, wskazać zaś należy, że dane zaszyfrowane *de facto* nie stanowią informacji, jawiąc się jako porcja kodu niezrozumiałego nawet dla komputera. Bez wątpienia, zaszyfrowana wiadomość (kierowana np. z wykorzystaniem poczty elektronicznej) zawiera w sobie ukryte informacje, jednak bez odszyfrowania, pozostają one niedostępne dla osoby, która podsłuchała tak zabezpieczony komunikat. W obydwu wskazanych wypadkach, dokonywane jest zatem przechwycenie nie tyle informacji, co danych.

Powyższe wątpliwości częściowo tracą swoje znaczenie w przypadku ataku polegającego na włamaniu się do systemu pośredniczącego w transmisji danych, np. systemu dostawcy usług sieciowych, bowiem w sytuacji tej zastosowanie znajdują regulacje kierowane przeciwko uzyskaniu bezprawnego dostępu do systemu. Czyn taki - choć może wpływać negatywnie na transmisję danych, nie jest wykonywany wobec samej transmisji, lecz danych przetwarzanych lokalnie wewnątrz jednego z atakowanych systemów. Przestępstwa tego typu przeanalizowane zostaną w części 4. rozdziału.

Istotną wątpliwość budzi wreszcie także kwestia uznania oprogramowania komputerowego za „informację”. O ile przytaczane regulacje międzynarodowe odnosząc się do „danych” jednoznacznie obejmują swoim zakresem także wszelkie przejawy ingerencji

---

[33] Więcej na temat tzw. *torrentów* oraz obsługującego technologię protokołu BitTorrent na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/BitTorrent.

w transmisję zawierającą skompilowany kod programu (bez wątpliwości kod źródłowy – a więc czytelny dla człowieka należy uznać za informację), o tyle zastosowana w polskim prawie kategoria „informacji" pozostawia w tym zakresie istotne niedomówienie. Przedstawiana wątpliwość jest tym bardziej uzasadniona, że na gruncie innych jednostek redakcyjnych Kodeksu karnego wykorzystywane są inne określenia, takie jak „dane informatyczne" (art. 268a - 269a Kk), czy wręcz „programy komputerowe" (art. 269b Kk), uprawniające stwierdzenie, że w odniesieniu do programów ustawodawca wykorzystuje określenia inne niż „informacje". Z punktu widzenia funkcjonalnego, a także konieczności zapewnienia zgodności regulacji krajowych z obowiązującymi regulacjami ponadnarodowymi, należy jednak skłaniać się w stronę uznania, że pod pojęciem „informacji" należy także rozumieć oprogramowanie.

Zastosowane w przepisie art. 267 § 1 sformułowanie „dostęp do informacji" powoduje penalizację już samej możliwości odczytu informacji[34], czyniąc prawnie irrelewantną kwestię, czy sprawca przestępstwa rzeczywiście zapoznał się z informacjami przechwyconymi w trakcie podsłuchu, czy też poprzestał na uzyskaniu samej możliwości dostępu do nich[35]. *De facto* rozwiązanie to rozszerza zakres ochrony gwarantowanej przez przepis, obejmując już nie tylko poufność informacji, ale także same zasady dostępu do niej. Z punktu zaś widzenia procesu karnego, przyjęty przepis istotnie upraszcza prowadzenie postępowania dowodowego.

Dla uznania, że uzyskanie dostępu do informacji w ramach podsłuchu transmisji danych nosi znamię „bezprawności", niezbędne jest stwierdzenie, że osoba podsłuchująca nie posiadała stosownego tytułu prawnego do uzyskania określonej informacji w czasie dokonywania czynu[36], w szczególności zaś nie została włączona do komunikacji przez jej pozostałe strony (np. nie została wskazana, jako adresat wiadomości *e-mail*)[37]. Zgodnie z ogólną charakterystyką przestępstwa, która zaprezentowana została na początku rozważań, także dla wystąpienia kodeksowej przesłanki „bezprawnego dostępu do informacji", nie jest przy tym istotne, czy podsłuchana informacja jest (lub była) dostępna publicznie w innym źródle, bowiem o poufnym charakterze transmisji decydują *de facto* same osoby wykonujące

34 W. Wróbel, op. cit., system LEX - komentarz do art. 267 k.k.

35 J. Piórkowska-Flieger w: T. Bojarski, A. Michalska-Warias, J. Piórkowska-Flieger, M. Szwarczyk, Kodeks karny. Komentarz, LexisNexis, wydanie 3, Warszawa 2009, s. 589.

36 Takie uprawnienie może wynikać w szczególności z funkcjonowania stosownej podstawy prawnej, np. zezwalające na pozyskiwanie określonych informacji w ramach wykonywanych czynności procesowych, por. A. Bojańczyk, Glosa do wyroku Sądu Najwyższego z 10 maja 2002 r., WA 22/02, Palestra 2003, Nr 7 – 8, czy też P. Kosmaty, Podsłuch komputerowy. Zarys problematyki, Prokurator 2008, Nr 4, przytaczam za M. Siwicki, op. cit., s. 131.

37 A. Lach, op. cit., system LEX - komentarz do art. 267 k.k.

transmisję. Jednocześnie, dla potwierdzenia bezprawności dostępu do informacji, nie ma także znaczenia fakt, czy uzyskana informacja była poszukiwana przez sprawcę, czy też jest dla niego w ogóle interesująca, czy przydatna[38]. W przypadku uzyskania dostępu do informacji lub też zapoznania się z nią wskutek błędu któregokolwiek systemu teleinformatycznego, w szczególności systemu osoby uzyskującej dostęp lub systemu, na którym przechowywane są dane zasoby, zapoznanie takie nie może być uznawane za bezprawne, wykluczając jednocześnie możliwość przypisania winy umyślnej osobie uzyskującej nieprzeznaczoną dla niej informację. Bezprawność naruszenia prywatności może zostać wyłączona także za zgodą komunikujących się stron, co w dzisiejszych czasach wydaje się być nadużywane przez pracodawców[39]. Monitorowanie pracy systemu komputerowego przybliżone zostanie w części 3. rozdziału, ponieważ nie wiąże się z przechwytywaniem występującej w sieci transmisji danych.

Zgodnie z przytoczonym brzmieniem art. 267 § 1, podsłuchiwanie transmisji danych w cyberprzestrzeni dokonywane jest na gruncie polskiej regulacji karnej, poprzez „podłączenie się do sieci telekomunikacyjnej"[40]. Przykładem takiej sieci w szczególności jest Internet[41], choć przytoczone sformułowanie nie stawia żadnych wymogów odnoszących się do rodzaju sieci, czy też jej zasięgu. Dla spełnienia wskazanej przesłanki nie ma zatem znaczenia, czy sprawca oraz cel (*ofiara)* cyberataku działają w ramach jednej klasy adresowej, czy też sieci dostarczanej przez tego samego operatora - wystarczające jest działanie poprzez sieć telekomunikacyjną, wiążące się z wykonywaniem transmisji danych. Z uwagi na konstrukcję językową przepisu, wystąpienie przesłanki „podłączenia się do sieci telekomunikacyjnej" wyklucza konieczność badania wystąpienia przesłanki „przełamania albo ominięcia" zabezpieczenia, co wiąże się z zastosowanym pomiędzy obiema przesłankami funktorem „lub", wywołującym funkcję alternatywy łącznej[42]. Od strony technicznej, podsłuchiwanie transmisji danych może jednak wiązać się zarówno z łamaniem, jak i omijaniem ewentualnych zabezpieczeń, mających na celu autentykację stron komunikacji, czy też przerabianie oznaczeń pakietów danych transmitowanych poprzez Internet.

Na tle zasygnalizowanych wyżej braków regulacji art. 267 § 1, niezwykle istotna staje

---

[38] M. Kalitowski w: Kodeks karny. Komentarz, pod red. M. Filara, LexisNexis , wyd. 2, Warszawa 2010, s. 1144.

[39] Wybrane formy nadużyć uprawnień w przedsiębiorstwie opisuje szeroko: W. Jasiński, Nadużycia w przedsiębiorstwie – przeciwdziałania i wykrywanie, Poltext, Warszawa 2013.

[40] W. Wróbel, op. cit., system LEX - komentarz do art. 267 k.k.

[41] J. Piórkowska-Flieger, op. cit., s. 588.

[42] *Ibidem*, s. 589.

się norma art. 267 § 3, która rozszerza zakres penalizacji odnoszącej się do podsłuchiwania transmisji danych na przypadki stosowania wszelkiego rodzaju oprogramowania lub urządzeń (zatem nie tylko systemów komputerowych), w celu uzyskania informacji[43]. Inaczej niż w przypadku regulacji art. 267 § 1, komentowany przepis § 3 nie wymaga uzyskania dostępu do informacji, zaś aktualizuje się już w momencie założenia lub posłużenia się narzędziem określonego rodzaju, z zamiarem bezprawnego uzyskania informacji. Co istotne, w odróżnieniu od redakcji art. 269b § 1 Kodeksu karnego, art. 267 § 3 nie wymaga aby stosowane urządzenia lub oprogramowanie były specjalnie stworzone lub przystosowane do popełniania określonych kategorii przestępstw, dopuszczając także karalność niegodziwego posługiwania się oprogramowaniem o w pełni legalnej funkcjonalności oraz pochodzeniu. W literaturze wielokrotnie podkreślany jest fakt, że cyberprzestępcy nierzadko wykorzystują te same programy służące do wykrywania luk w bezpieczeństwie, co administratorzy serwerów. Różnica dzieląca atakujących od obrońców polega w tym wypadku jedynie na sposobie wykorzystania ujawnionych informacji o podatnościach[44]. Przyjęta redakcja § 3 powoduje, że przestępstwo ujęte w tym przepisie ma charakter formalny, a więc dla jego zaistnienia nie jest istotne wystąpienie żadnego określonego skutku - przenosząc się do obszaru cyberprzestrzeni, nie ma znaczenia, czy przeprowadzony atak okazał się skuteczny. Tym samym, w sytuacjach faktycznych opisujących przypadki podsłuchiwania transmisji danych, które wymykają się penalizacji karnej na podstawie art. 267 § 1 z uwagi na przechwycenie jedynie porcji danych - nie zaś informacji, potencjalne zastosowanie znajdować będzie przepis art. 267 § 3, bowiem każde działanie w komputerze - nawet bez stosowania specjalistycznego oprogramowania, dokonywane jest przy użyciu urządzenia lub programu (choćby komputera z zainstalowanym systemem operacyjnym). Niezbędne w tym wypadku będzie jednak udowodnienie, że sprawca przestępstwa działał z zamiarem uzyskania informacji - a nie np. w celu zbadania poziomu bezpieczeństwa zaatakowanego systemu, co może nastręczać problemów dowodowych[45].

Zbieg art. 267 § 1 i 3 oraz art. 269b § 1 oznacza możliwość stosowania podwójnej kwalifikacji karnej dla czynów polegających na podsłuchiwaniu transmisji, w ramach której przekazywane są hasła lub kody dostępu. Transmisja taka wykonywana jest nie tylko w przypadku wysłania hasła lub kodu np. w treści poczty elektronicznej, ale przede wszystkim, w trakcie wykorzystywania takiego hasła lub kodu do zalogowania się do

---

[43] W. Wróbel, op. cit., system LEX - komentarz do art. 267 k.k.
[44] A. Adamski, Cyberprzestępczość..., op. cit., s. 60.
[45] Problematyczność dowodzenia określonego zamiaru w sieci podnosi m. in. A. Adamski, Prawo karne..., op. cit., s. 58.

określonej usługi sieciowej - np. do systemu bankowego. Co warto zauważyć, posługiwanie się wszelkiego rodzaju hasłami w cyberprzestrzeni występuje najczęściej przypadkach transmisji danych, w których użytkownik - człowiek, występuje tylko po jednej stronie komunikacji danych. Odbiorcą wprowadzanego hasła lub kodu w tego typu sytuacjach najczęściej staje się natomiast zautomatyzowany system. Porównując obie przytoczone regulacje, przepis art. 269b § 1 nie wprowadza żadnych dodatkowych przesłanek karalności pozyskiwania „haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej", tak jak czyni to art. 267, zatem nie jest w przypadku stosowania art. 269b § 1 niezbędne badanie np. tego czy, określony czyn dokonano podłączając się do sieci, czy też przełamane lub ominięte zostały jakiekolwiek zabezpieczenia. Wątpliwości rysują się jednak ponownie na tle kwestii przechwytywania części haseł oraz haseł zaszyfrowanych. W związku z wprowadzonym w przepisie sformułowaniem definiującym hasła oraz kody, jako „dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej", należy bowiem zauważyć, że hasło niekompletne, czy tez zakodowane nie zezwala na uzyskanie takiego dostępu. Ponieważ szyfrowanie połączeń, w trakcie których przekazywane są hasła staje się dziś standardem (włączenie szyfrowania nie wymaga czynnego udziału ze strony użytkownika), podstawowym sposobem przestępnym uzyskiwania haseł staje się dziś tzw. *phishing*, stanowiący sztandarowy przykład techniki oszustwa komputerowego.

W ramach analizy prawno-porównawczej, na tle powyższych wątpliwości szczególnie istotne wydaje się w tym miejscu odwołanie do regulacji amerykańskich, nastawionych na zwalczanie bezprawnego podsłuchiwania transmisji danych. Zgodnie z sekcją 2511 (1)(a) tytułu osiemnastego U.S.C[46] - zatytułowaną „Zakaz przechwytywania oraz ujawniania komunikatów przekazywanych kablowo, ustnie lub elektronicznie"[47], ustawowej penalizacji poddane zostały działania polegające na:

> „(a) umyślnym przechwytywaniu, usiłowaniu przechwycenia lub nakłanianiu innej osoby do przechwytywania lub usiłowania przechwycenia jakiejkolwiek kablowej, ustnej lub elektronicznej komunikacji;"[48].

Zgodnie zaś z sekcją 2510 (4), pojęcie „przechwytywania danych" zdefiniowane zostało

---

[46] *United States Code*. Oryginalny tekst sekcji 2511 ustawy dostępny na stronie internetowej pod adresem: http://www.law.cornell.edu/uscode/text/18/2511.

[47] W oryginale: „*Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited*". Tłumaczenie własne.

[48] W oryginale: „*(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;*". Tłumaczenie własne.

w ustawie amerykańskiej, jako:

„dźwiękowe lub dokonane w innej formie pozyskanie zawartości jakiejkolwiek kablowej, elektronicznej lub ustnej komunikacji, dokonywane przy wykorzystaniu jakiegokolwiek elektronicznego, mechanicznego lub innego urządzenia."[49].

Scalając obie przytoczone jednostki redakcyjne w jedną normę prawną, na gruncie amerykańskiego prawa federalnego, szerokim zakresem penalizacji objęty jest każdy czyn polegający na umyślnym oraz bezprawnym przechwytywaniu zawartości jakiejkolwiek komunikacji przy zastosowaniu w tym celu dowolnego urządzenia zdolnego do przechwycenia komunikacji[50]. Dla zaistnienia stypizowanego w ten sposób czynu nie jest zatem istotne, jakie dane zostały przechwycone, jak również to czy są kompletne i nadają się do wykorzystania przez atakującego. Co więcej, dla spełnienia hipotezy zrekonstruowanej normy prawnej nie ma znaczenia, czy przechwycone dane zostały w ogóle odczytane. Sankcjonowany bowiem jest w tym wypadku już sam fakt przechwytywania zawartości komunikacji, nie zaś dopiero fakt naruszenia jej poufności[51]. Zgodnie z przyjętym w USA orzecznictwem za bezprawne przechwytywanie danych nie można natomiast uznawać technicznych zasad rządzących systemami teleinformatycznymi, np. odnoszących się do sposobu przekazywania wysyłanej poczty elektronicznej pomiędzy kolejnymi węzłami pośredniczącymi. Czasowe przetwarzanie zawartości komunikacji nie jest w tym wypadku uważane za „przechwytywanie", choć pojęciem tym obejmuje się w amerykańskiej praktyce sądowej również działania polegające na uzyskiwaniu dostępu do cudzych komunikatów nagranych na jego komputerze - np. kopii wysłanych i otrzymanych wiadomości, przechowywanych lokalnie w programie pocztowym[52].

Podsumowując wcześniejsze rozważania dotyczące krajowej regulacji karnej penalizującej podsłuchiwanie transmisji danych, należy podnieść konieczność dostosowania jej brzmienia do postanowień Konwencji Rady Europy o cyberprzestępczości oraz w zakresie stosowanej siatki terminologicznej - także Decyzji Ramowej Rady Unii Europejskiej w sprawie ataków na systemy informatyczne[53] oraz aktualnie zastępującej ją Dyrektywy

---

[49] W oryginale: *„"intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device*". Tłumaczenie własne.

[50] Zgodnie z sekcją 2510 (5) tytułu osiemnsastego USC pod pojęciem "elektronicznego, mechanicznego lub innego urządzenia" należy rozumieć każde urządzenie lub aparat, które może zostać wykorzystane do przechwycenia kablowej, ustnej lub elektronicznej komunikacji. W oryginale: „(*5) "electronic, mechanical, or other device*" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication". Tłumaczene własne.

[51] H. M. Jarrett, M. W. Bailie, E. Hagen, S. Eltringham, *Prosecuting Computer Crimes*, Wydawnictwo Kształcenia Prawnego (Office of Legal Education Executive Office for United States Attorneys), s. 60 i nast.

[52] *Ibidem*, s. 63 i nast.

[53] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy

Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne[54] – zawierającej analogiczne w tym zakresie rozwiązania prawne. Nieprecyzyjne różnicowanie na gruncie Kodeksu karnego pojęć „informacja" oraz „dane", rodzi istotne problemy interpretacyjne o doniosłości praktycznej. Czy umyślne podsłuchanie jedynie fragmentu transmisji (z zamiarem sprawcy obejmującym właśnie tylko fragment transmisji) może być oceniane choćby, jako usiłowanie popełnienia przestępstwa, które kierowane musi być przeciwko informacji? Podobnie, jak należy oceniać przechwycenie informacji zaszyfrowanej, która nie zostaje następnie poddana żadnej próbie rozkodowania? Ostatecznie, w jaki sposób jednoznacznie udowodnić przestępcy zamiar zdobycia informacji, który niezwykle łatwo przykryć chęcią zbadania stosowanych zabezpieczeń? Prezentowany brak precyzji w zakresie określenia przedmiotu przestępstwa oceniać trzeba, jako wyraz niepokojącej nierzetelności ustawodawcy, bowiem przedstawiane wątpliwości dotyczą podstawowej dla prawa karnego kwestii zasięgu penalizacji. Przyjęta regulacja nie zapewnia także należytego poziomu spójności z art. 49 Konstytucji oraz 159 ustawy - Prawo telekomunikacyjne. Jako postulat *de lege ferenda* należy wskazać zasadność rozwiązania naświetlanego problemu poprzez dostosowanie terminologii do tej stosowanej w doktrynie międzynarodowej oraz umowach międzynarodowych, a także wprowadzenie jednoznacznej definicji pojęcia „informacja". Przyszła regulacja winna także penalizować każdy przejaw podsłuchiwania transmisji danych - w tym wszelkiego rodzaju haseł, niezależnie od tego, czy dane te składają się na informacje lub też, czy nadają się do odczytu. Z uwagi na znaczenie oraz szkodliwość przestępstwa podsłuchiwania transmisji danych, godzącego przecież w prawa gwarantowane na poziomie konstytucyjnym, przyjęty w komentowanych przepisach wnioskowy tryb ścigania, winien być również zastąpiony trybem ścigania z urzędu. *De lege lata*, w przypadkach wymykających się regulacji art. 267 § 1 winien być zaś stosowany art. 267 § 3 oraz 269b § 1. Ostatecznie, porównując rozwiązania krajowe z przytoczonymi regulacjami amerykańskimi nie sposób nie podkreślić różnic w filozofii, która przyświecała tworzeniu wszystkich cytowanych przepisów. Podczas, gdy regulacje polskie kierowane są na penalizację precyzyjnie określonych stanów faktycznych, przepisy amerykańskie zakreślają niezwykle szeroki obszar poddany kontroli prawnej.

Przestępstwa związane z tworzeniem oraz udostępnianiem narzędzi służących do

---

informatyczne, Nr 2005/222/WSiSW.

[54] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW. Pełny tekst dyrektywy dostępny na stronie internetowej pod adresem: http://bip.ms.gov.pl/Data/Files/_public/bip/prawo_eu/ue2/dyrektywa-2013_40_ue-o-cyberprzestepczosci.pdf.

popełniania cyberprzestępstw - w tym służących do prowadzenia podsłuchu, przybliżone zostaną w części 5. rozdziału.

2. Modyfikowanie lub zakłócanie treści transmisji

Drugim z wymienionych cyberprzestępstw, które kierowane są przeciwko transmisji danych, jest przestępstwo bezprawnego modyfikowania lub zakłócania treści transmisji. Inaczej niż w przypadku wskazanego wyżej podsłuchu komputerowego - który narusza poufność danych, modyfikacja lub zakłócanie danych wymierzone są przeciwko integralności (autentyczności) oraz dostępności przekazu. Pomimo różnicy w określeniu przedmiotu ataku, pomiędzy oboma przestępstwami zachodzi swoiste podobieństwo genetyczne. Z uwagi na analogiczny sposób działania sprawców obu wymienionych kategorii cyberprzestępstw, modyfikowanie lub zakłócanie treści może wiązać się z jednoczesnym odczytywaniem zaburzanych pakietów danych, łącząc się wówczas funkcjonalnie z podsłuchem. Połączony w ten sposób atak wykonywany jest w konsekwencji jednocześnie przeciwko integralności, jak i poufności transmisji. W przypadku stwierdzenia możliwości zapoznania się przez atakującego z treścią nieprzeznaczonych dla niego danych (poddawanych modyfikacji) należy zatem mówić o zbiegu przestępstw bezprawnego podsłuchu oraz nieuprawnionej modyfikacji treści transmisji.

Od strony technicznej, możliwość modyfikacji lub zatrzymywania transmitowanych danych, wymaga uprzedniego przejęcia kontroli nad samą transmisją danych. W celu tym stosowane są analogiczne metody ataku, jak w przypadku bezprawnego podsłuchiwania transmisji, np. zaprezentowany wyżej atak typu *man-in-the-middle* wykorzystujący technikę *IP spoofing'u*, czy też sygnalizowane ataki przeciwko węzłom pośredniczącym (*vide* część I.1 rozdziału). Zatruwanie tablic DNS może być z kolei wykorzystywane do zakłócania transmisji danych lub też przejmowania nad nią kontroli na wielką skalę (np. dla odcięcia od poczty elektronicznej całej instytucji państwowej)[55].

Wprowadzanie zmian w przesyłanych danych, w tym też obejmujące ich całościową podmianę, wiąże się z koniecznością włączenia się do strumienia transmisji danych oraz uzyskania możliwości dalszego przesyłania danych zmodyfikowanych lub niekompletnych. Analogicznie, jak w przypadku podsłuchu, całość działań przeprowadzana jest w sposób, który zapewnia, że komunikujące się strony pozostają w całkowitym przekonaniu

[55] Poprzez zatrucie DNS możliwe jest wprowadzenie swoistego objazdu, kierującego pocztę elektroniczną do nieistniejącego odbiorcy. Poczta wysyłana na tak przekierowany adres nie dociera do odbiorcy, często wracając do swojego nadawcy.

o autentyczności przekazu. Innymi słowy, otrzymywane przez ofiary ataku dane muszą wyglądać na pochodzące z oryginalnego źródła oraz nie nosić żadnych śladów modyfikacji. Warto w tym miejscu przypomnieć, że stronami komunikacji w cyberprzestrzeni mogą być nie tylko użytkownicy, ale także w pełni zautomatyzowane systemy, co rozszerza potencjalny zakres transmisji, które mogą stać się przedmiotem bezprawnego ataku. Przykładowo, bezprawnej modyfikacji treści transmisji poddane mogą zostać dane w postaci *loginu* i hasła, które kierowane są przez użytkownika do systemu kontroli dostępu określonej usługi sieciowej. Celem takiego ataku może być chęć zablokowania oraz przejęcia kontroli nad kontem użytkownika (kilkukrotne wpisanie „za uprawnionego użytkownika" błędnego hasła może spowodować np. czasowe zablokowanie jego adresu IP). Wszystkie ze wskazywanych działań mogą być wykonywane zarówno indywidualnie (*ręcznie*) przez samego cyberprzestępcę, jak również być wynikiem działania przygotowanego przez niego oprogramowania, mogącego w sposób automatyczny nie tylko dokonywać operacji na danych, ale także wyszukiwać kolejne ofiary cyberataków.

W odniesieniu do transmisji bezprzewodowej, naruszanie dostępności komunikacji możliwe jest także poprzez fizyczne zakłócanie rozgłaszanych w eterze fal radiowych. Stosowane w tym zakresie urządzenia - nazywane z języka angielskiego *jammerami*[56], pozwalają na zagłuszanie fal, uniemożliwiając np. stosowanie *routerów* bezprzewodowych, czy telefonów komórkowych na określonym obszarze. W polskim porządku prawnym, działania tego typu wykonywane mogą być wyłącznie przez podmioty uprawnione ustawowo[57], które w swoim zakresie kompetencyjnym posiadają zadania związane z ochroną bezpieczeństwa ludzi oraz państwa.

Szczególne przykłady ataków, które mogą zostać wykorzystane również do zakłócania transmisji danych (ataki typu *Dos* oraz *Ddos* - w których jako narzędzie przestępne wykorzystywana jest sama transmisja danych) przybliżone zostaną, zgodnie z przyjętą systematyką, w kolejnym punkcie rozdziału.

Przechodząc do analizy prawnej przestępstwa modyfikacji lub zakłócania transmisji danych, w pierwszej kolejności ponownie warto odwołać się do postanowień Konwencji o cyberprzestępczości, gdzie komentowane przestępstwo określone zostało mianem „ingerencji w dane"[58] (w oficjalnym przekładzie - „Naruszenie integralności danych").

---

[56] Więcej na ten temat na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Radio_jamming.

[57] Art. 178 ust. 3 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800). Pośród organów uprawnionych do stosowania poruszanego rozwiązania przepis wymienia w szczególności Policję, Agencję Bezpieczeństwa Wewnętrznego oraz Biuro Ochrony Rządu.

[58] W oryginale: „*data interference*".

Zgodnie z art. 4 ust. 1 Konwencji:

> „Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego, popełnionego umyślnie czynu polegającego na bezprawnym niszczeniu, usuwaniu, uszkadzaniu, modyfikowaniu lub utrudnianiu dostępu do danych komputerowych."[59]

Przyjęta przez autorów Konwencji konstrukcja legislacyjna przepisu odnosi prezentowaną normę do każdego przejawu bezprawnego niszczenia, usuwania, uszkadzania, modyfikowania, czy utrudniania dostępu do danych komputerowych - bez względu na charakter danych będących przedmiotem ataku, jak również miejsce ich przetwarzania (w oficjalnym tłumaczeniu katalog ten został ujęty, jako „niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych"). W efekcie, przytoczony przepis chroni dane komputerowe niezależnie od tego, czy:

1) atakowane dane są w jakikolwiek sposób istotne lub interesujące dla cyberprzestępcy lub też w ogóle nadają się do odczytania lub wykorzystania przez niego w jakikolwiek sposób;
2) atakowane dane są w jakikolwiek sposób istotne dla ich właściciela lub osób uprawnionych do ich przetwarzania;
3) atakowane dane przetwarzane są lokalnie, to jest wewnątrz komputera, czy też podlegają transmisji za pośrednictwem sieci teleinformatycznych (publicznych, prywatnych, przewodowych, bezprzewodowych, itd.); a także,
4) atakowane dane stanowią wytwór człowieka, czy też maszyny (np. automatycznie gromadzone *logi* systemowe, stanowiące swoiste dzienniki funkcjonowania systemu).

Co również warto zaznaczyć, przepis art. 4 Konwencji nie wprowadza żadnego różnicowania na dane „cywilne" oraz dane „państwowe", obejmując swoim zakresem penalizacji obydwie te kategorie jednocześnie.

Obok ogólnego wskazania przedmiotu wykonawczego ataku, na gruncie przepisu Konwencji szeroko zakreślony został także katalog form niedopuszczalnego oddziaływania na dane. Zgodnie z przyjętą regulacją, penalizacji poddane zostały wszelkie czynności polegające na niszczeniu, usuwaniu, uszkadzaniu, modyfikowaniu oraz utrudnianiu dostępu do danych komputerowych. Zgodnie z Raportem Wyjaśniającym do Konwencji, przyjęty katalog miał za zadanie zapewnienie zasobom komputerowym - to jest danym oraz

---

[59] W oryginale: „*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*". Tłumaczenie własne.

programom, takiej samej ochrony, jakiej poddawane są rzeczy materialne[60]. Przywołany Raport niejako uzupełnił postanowienia Konwencji wskazując również, że pod pojęciem „tłumienie” należy rozumieć wszelkie działania mające na celu utrudnienie lub uniemożliwienie uprawnionego dostępu do określonego zasobu komputerowego[61], co w praktyce może odnosić się np. do uszkodzenia rozszerzenia pliku jednak bez naruszania jego zawartości, czy też uszkodzenia informacji o sposobie podziału dysku twardego komputera na partycje - również niewiążącego się z modyfikacjami zapisu samych danych. W obydwu tych przypadkach, pomimo braku modyfikacji zawartości poszczególnych plików komputerowych zapisanych na informatycznych nośnikach danych dochodzi do uniemożliwienia osobie uprawnionej odczytu zaatakowanych danych, jak też ich automatycznego przetworzenia przez system.

Bazując na postanowieniach Konwencji Budapesztańskiej, nieuprawnione modyfikowanie lub uszkadzanie danych spenalizowane zostało także w przepisach Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[62], w której art. 4 usankcjonowano - w sposób zbieżny do wskazanej wyżej regulacji Konwencji o cyberprzestępczości, że:

> „Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślne bezprawne usunięcie, uszkodzenie, pogorszenie, zmiana, zatajanie lub uczynienie niedostępnymi danych komputerowych w systemie informatycznym jest karane jako przestępstwo, kiedy dokonywane jest bezprawnie, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.”[63]

Przyjęte postanowienie Decyzji Ramowej zostało następnie przetransponowane do przepisu art. 5 Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne[64], otrzymując ostatecznie brzmienie:

> „Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne

[60] Pkt 60 Raportu Wyjaśniającego. W oryginale: „*The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage.*”. Tłumaczenie własne.

[61] Pkt 61 Raportu Wyjaśniającego. W oryginale: „ *Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored.*”. Tłumaczenie własne.

[62] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW.

[63] Art. 4 Decyzji Ramowej Rady Unii Europejskiej w sprawie ataków na systemy informatyczne. Przytoczony fragment pochodzi z oficjalnej polskiej wersji językowej dokumentu.

[64] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW. Pełny tekst dyrektywy dostępny na stronie internetowej pod adresem: http://bip.ms.gov.pl/Data/Files/_public/bip/prawo_eu/ue2/dyrektywa-2013_40_ue-o-cyberprzestepczosci.pdf.

i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi, było karalne jako przestępstwo, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.”

Analogicznie, jak w przypadku postanowień Konwencji o cyberprzestępczości, zakres przedmiotowy przytoczonego przepisu Decyzji Ramowej oraz Dyrektywy określony został szeroko, bez wprowadzania jakichkolwiek ograniczeń, które odnosiłyby się do właściwości atakowanych danych, systemów, czy też sprawcy lub ofiary cyberataku. Z uwagi na zbieżność regulacji przyjętych w Decyzji Ramowej i Dyrektywie oraz Konwencji, pełne zastosowanie znajdują tu wcześniejsze uwagi, z zastrzeżeniem jednak kwestii językowej dot. sposobu tłumaczenia angielskiego wyrażenia „*suppresion*”. Na gruncie polskiej wersji językowej art. 4 Decyzji Ramowej wyraz ten został przetłumaczony, jako „zatajanie” – podczas, gdy w przepisach Dyrektywy tłumaczenie to zastąpiono zwrotem „eliminacja”. W kontekście tłumaczenia własnego, które przeprowadzone zostało przez autora niniejszej pracy na gruncie postanowień Konwencji o cyberprzestępczości – pojęcie „*suppresion*” przetłumaczono wprost, jako „tłumienie”, odwołując się wówczas do Raportu Wyjaśniającego do Konwencji o cyberprzestępczości. W dokumencie tym pojęcie „*suppresion*” zostało zdefiniowane, jako oznaczające wszelkie formy utrudniania lub uniemożliwiania uzyskania uprawnionego dostępu do danych komputerowych - co w ocenie Autora niniejszej dysertacji nie wiąże się bezpośrednio z polską konotacją wyrazu „zatajać”, czy też w szczególności „eliminować”. Porównując redakcję analizowanych przepisów, należy uznać, że rozbudowany, złożony zapis Decyzji Ramowej w brzmieniu „*suppression or rendering inaccessible of computer data*” („zatajanie lub uczynienie niedostępnymi danych komputerowych”) oraz analogiczny zapis Dyrektywy, stanowią nadmiarowe rozwinięcie samodzielnego wyrażenia „*suppresion*”. Przyjęte natomiast w polskiej wersji językowej Dyrektywy tłumaczenie tego zwrotu jako „eliminacja” uznać należy za mylące oraz w istocie dublujące znamię „usuwania danych”.

Na gruncie polskich regulacji krajowych, przestępstwo nieuprawnionego modyfikowania lub uszkadzania danych transmitowanych za pośrednictwem sieci podlega kwalifikacji karnej z dwóch przepisów Kodeksu karnego, to jest art. 268a oraz 269. Przepisy te przyjmują następujące brzmienie:

„Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Art. 269. § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.”.

Podobnie, jak w przypadku wskazanych wyżej regulacji międzynarodowych, pochodzących z Konwencji o cyberprzestępczości oraz Decyzji Ramowej Rady Unii Europejskiej, przytoczone przepisy Kodeksu karnego nie rozdzielają penalizacji nieuprawnionej modyfikacji danych na przypadki odnoszące się do danych przekazywanych za pośrednictwem sieci, jak i tych przetwarzanych lokalnie - obejmując obie te sytuacje jednocześnie[65]. Zgodnie z przyjętym podziałem cyberprzestępstw, prowadzona w tym miejscu analiza ograniczona jest do przybliżenia kwalifikacji cyberataków dokonywanych wobec transmisji danych, pozostawiając przypadki modyfikacji danych przetwarzanych lokalnie (to jest wewnątrz komputera) dla części 4 niniejszego rozdziału.

Zestawiając oba przytoczone wyżej przepisy art. 268a oraz 269 Kodeksu karnego w jednolitą normę prawną sankcjonującą nieuprawnione modyfikowanie lub usuwanie danych transmitowanych poprzez sieci, ogólnie stwierdzić należy, że na gruncie polskiego prawa zabroniony jest każdy czyn kierowany przeciwko integralności lub dostępności danych przesyłanych pomiędzy dowolnymi systemami, polegający na niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostępu do danych informatycznych, jak też każdy czyn, który w istotnym stopniu zakłóca lub też uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych[66]. Zgodnie z przyjętą regulacją, wskazane

[65] P. Kozłowska-Kalisz, Kodeks karny. Komentarz, pod red. M. Mozgawa, M. Budyn-Kulik, P. Kozłowska-Kalisz, M. Kulik, WK, 2015, system LEX - komentarz do art. 268a.

[66] A. Lach, op. cit., system LEX - komentarz do art. 267 k.k.

działania ścigane są na wniosek pokrzywdzonego oraz podlegają maksymalnej sankcji do 5 lat pozbawienia wolności. W przypadkach, gdy cyberatak kierowany jest przeciwko danym o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub też instytucji państwowej albo samorządu terytorialnego - czyn taki, z wyłączeniem jednak znamienia „utrudnienia dostępu do danych informatycznych", ścigany jest z urzędu oraz podlega maksymalnej karze 8 lat pozbawienia wolności, niezależnie od stopnia zakłócenia automatycznego przetwarzania danych.

Zastosowany w obydwu jednostkach redakcyjnych zwrot „automatyczne przetwarzanie danych", nie doczekał się swojej definicji ustawowej na gruncie Kodeksu karnego, pomimo wieloletniego już sygnalizowania w doktrynie problemu określenia znaczenia tego pojęcia[67]. Zgodnie z definicją „przetwarzania danych" pochodzącą z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[68], przetwarzaniem danych są:

> „jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych".

Zgodnie zaś z przepisami ustawy z dnia 5 sierpnia 2010 r. o ochronie niejawnych, pod pojęciem przetwarzania informacji niejawnych rozumie się:

> „wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie".

Jak wynika z przytoczonych definicji ustawowych, pojęcie „przetwarzania" stanowi w istocie kategorię zbiorczą, obejmującą wszelkie operacje, jakie potencjalnie można wykonywać na danych lub informacjach. W takim ujęciu każde działanie wykonywane na danych, o których stanowią przepisy Kodeksu karnego, winno być uznawane za „przetwarzanie" - niezależnie nawet od tego, czy dany rodzaj operacji został już wymyślony, czy dopiero pojawi się w przyszłości, co ma niebagatelne znaczenie dla zakresu ochrony danych informatycznych, które przetwarzane są - a w tym segregowane, w sposób automatyczny przez systemy teleinformatyczne. Odnosząc przytoczone definicje do regulacji Kodeksu karnego, należy jednak zwrócić uwagę na swoistą niekompatybilność materii ustawowej. Kodeks karny, określając przesłanki przestępstw określonych w art. 268a oraz 269 posługuje się zwrotem „automatyczne przetwarzanie, gromadzenie lub przekazywanie danych", sugerującym, że na

---

[67] Np. A. Adamski, Prawo karne komputerowe, CH Beck, Warszawa 2000, s. 79 i nast.
[68] Dz. U. Nr 133, poz. 883, z późn. zm.

gruncie jego regulacji pojęcia „gromadzenie” oraz „przekazywanie” zostały wyłączone z zakresu wyrażenia „przetwarzanie”. W przeciwnym wypadku, obie wyjęte operacje byłby poprzedzone w redakcji przepisu zwrotem „w szczególności”. Proste odniesienie definicji pochodzących z ustaw o ochronie danych osobowych oraz o ochronie informacji niejawnych do przepisów Kodeksu karnego obarczone jest w efekcie błędem logicznym, powodującym konieczność przyjęcia założenia, że ustawodawca nieracjonalnie (a zatem wbrew założeniom Konstytucji) powtórzył wyrażenia wchodzące w skład przewidzianego obok pojęcia. Jednoznaczne rozwiązanie prezentowanego problemu wymaga wprowadzenia Kodeksowej definicji „przetwarzania danych”.

Przybliżając przepisy karne, regulacja art. 268a stanowi bezpośrednie odzwierciedlenie implementowanych postanowień Konwencji Budapesztańskiej oraz analogicznych rozwiązań przyjętych na gruncie Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne. Przepis art. 268a obejmuje swoim zakresem przedmiotowym każdy przypadek modyfikacji danych[69], które transmitowane są za pośrednictwem sieci, niezależnie od przyjętej przez cyberprzestępcę metody działania, jak również charakteru samych danych[70] - w tym, czy dane dostępne były wyłącznie dla indywidualnie określonych osób, czy też publicznie np. na otwartej stronie internetowej. Dla ukonstytuowania tak stypizowanego przestępstwa nie jest zatem istotne, czy zaatakowane dane mają jakiekolwiek znaczenie, czy to dla cyberprzestępcy, czy też ofiary cyberataku, jak również to, czy wiążą się z nimi jakiekolwiek prawa majątkowe lub osobiste. Nie ma znaczenia również fakt, czy atakowane dane zostały wytworzone bezpośrednio przez człowieka, czy też automatycznie przez dowolny system komputerowy (np. dane obejmujące informacje o adresach IP, z których łączono się z daną stroną internetową - tzw. *logi*). Wreszcie, poza znamionami przepisu pozostaje także kwestia, czy zaatakowane dane mogą zostać w jakikolwiek sposób odzyskane przez ofiarę, czy też uległy bezpowrotnej utracie (np. czy ofiara cyberataku posiada kopię zapasową zniszczonych w trakcie transmisji danych). Wszystkie wymienione w przepisie znamiona czynu karalnego mogą jednocześnie być wykonywane bezpośrednio przez sprawcę cyberataku, jak również stanowić efekt działania umyślnie uruchomionego przez niego oprogramowania wykonującego bezprawne operacje w sposób zautomatyzowany, np. wirusa komputerowego. Wprowadzenie do komentowanego przepisu alternatywnej przesłanki „zakłócenia w istotnym stopniu lub też uniemożliwienia automatycznego przetwarzania, gromadzenia lub

[69] M. Siwicki, op. cit., s. 142 i nast.
[70] P. Kozłowska-Kalisz, op. cit., system LEX - komentarz do art. 268a.

przekazywania danych", pozwala na jednoznaczne objęcie przedmiotowym zakresem regulacji karnej także tych przypadków modyfikacji danych, które nie odnoszą się bezpośrednio do samej zawartości atakowanych plików, np. treści uszkadzanych dokumentów, zaś wykonywane są wobec swoistych *meta*-danych, wykorzystywanych przez komputery w trakcie przetwarzania danych informatycznych (np. prosta zmiana rozszerzenia pliku z .doc na .pdf powodująca niemożliwość jego otwarcia w programie przypisanym do danego typu plików w systemie operacyjnym, czy też zmiana tablicy znaków zniekształcająca sposób wyświetlania treści dokumentu). Za „istotne" zakłócenie automatycznej pracy systemu należy uznawać w szczególności zakłócenie podstawowych funkcji systemu, wpływające negatywnie na realizację przez niego usług na rzecz użytkownika lub zdolności do komunikowania z innymi systemami[71]. Z uwagi na różnorodność systemów, ich architektur oraz funkcjonalności, przeprowadzanie oceny, czy zakłócenie działania systemu rzeczywiście było istotne, musi być dokonywane w kontekście konkretnego systemu. Z punktu widzenia zasad tworzenia prawa, pozostawienie w przepisie przymiotnika „istotny" bez jakiegokolwiek przybliżenia jego znaczenia, uznać należy za błąd legislacyjny, zmniejszający faktyczną skuteczność analizowanej normy prawnej.

Zgodnie z art. 269 Kodeksu karnego, szczególną regulacją objęte zostały przypadki nieuprawnionego modyfikowania danych wrażliwych z punktu widzenia funkcjonowania oraz bezpieczeństwa państwa. Rozwiązanie takie - niewystępujące normatywnie na gruncie Konwencji o cyberprzestępczości, jak też przywoływanej wcześniej Decyzji Ramowej Rady Unii Europejskiej w sprawie ataków na systemy informatyczne oraz zastępującej jej Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne[72], stanowi odpowiedź na konieczność zapewnienia szczególnej ochrony określonym kategoriom systemów, należących w szczególności do zasobów infrastruktury krytycznej państwa. Wprowadzony do Kodeksu rozdział pozwolił także na zróżnicowanie trybu, w jakim ścigane są komentowane przestępstwa z art. 268a oraz 269 - o ile modyfikacja danych istotnych dla państwa podlega ściganiu z urzędu oraz zagrożona jest karą surowszą, o tyle w pozostałych przypadkach decyzja o ściganiu sprawcy pozostawiona została ofierze cyberataku, uprawnionej do złożenia wniosku o ściganie, inicjującego postępowanie „z urzędu". Z uwagi na specyfikę zwalczania

[71] Wskazówka ta podana została w pkt 67 Raportu Wyjaśniającego do Konwencji o cyberprzestępczości. Raport dostępny jest na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

[72] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

przestępczości komputerowej oraz konieczność posiadania specjalistycznej wiedzy informatycznej w tym zakresie, udział profesjonalnie przygotowanych organów ścigania w toku całego postępowania, uznać należy za element niezbędny dla faktycznej realizacji celów, jakie stawiane są przed procesem karnym.

Z uwagi na podobną budowę przepisów art. 268a oraz 269 Kodeksu karnego, wcześniejsze uwagi, które poczynione zostały w odniesieniu do typu podstawowego przestępstwa nieuprawnionego modyfikowania danych, w dużej mierze znajdują swoje zastosowanie także w przypadku charakterystyki przestępstwa kierowanego przeciwko danym „państwowym", stypizowanego w art. 269 Kodeksu karnego. Odrębnej analizy wymagają jednak dwie istotne różnice dzielące wskazane przepisy.

W pierwszej kolejności zauważyć należy, że w przypadku regulacji kwalifikowanego typu przestępstwa modyfikowania danych, odnośny przepis art. 269 Kodeksu karnego pozbawiony został - w stosunku do przepisów art. 268a, przesłanki „utrudniania dostępu do danych informatycznych" (stanowiącej element anglojęzycznego pojęcia „*suppresion*"). Przyjęte rozwiązanie, osłabiające w istocie zakres ochrony systemów krytycznych dla funkcjonowania państwa, uznać należy za pozbawione uzasadnienia merytorycznego. Oba komentowane przepisy Kodeksu karnego, to jest art. 268a oraz 269, charakteryzują w istocie ten sam czyn - nieuprawnione modyfikowanie danych, kładąc główny nacisk na zróżnicowanie sankcji karnych w zależności od rodzaju atakowanych danych[73]. Opierając się na dogmacie racjonalnego ustawodawcy, wprowadzona do art. 269 zmiana, oznacza jednak umyślne zróżnicowanie przez ustawodawcę katalogów skutków cyberataku, które objęte są penalizacją w myśl przepisów art. 268a oraz 269 Kodeksu karnego. Przepis szczególny zapewnia tym samym słabszą ochronę w zakresie sankcjonowanych skutków ataku. W nawiązaniu do wcześniejszych rozważań dotyczących znaczenia przesłanki „utrudniania dostępu do danych informatycznych", warto przypomnieć, że przesłanka ta pozwala na jednoznaczne objęcie penalizacją tych cyberataków, w następstwie których uszkadzane są swoiste *meta*-dane, nie zaś sama treść transmitowanych dokumentów (lub szerzej - zawartość przesyłanych plików). Należy zauważyć, że pomimo szeroko ujętego zakresu przedmiotowego przesłanki „zakłócenia lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania danych", ograniczona redakcja przepisu art. 269 Kodeksu karnego utrudnia jednoznaczne objęcie jego zakresem przedmiotowym np. prostego ataku polegającego na nieuprawnionym przenoszeniu plików pomiędzy katalogami. Przeniesienie

[73] A. Lach, op. cit., system LEX - komentarz do art. 267 k.k.

takie nie musi bowiem wiązać się z zaburzeniem automatycznego przetwarzania danych (automatycznego - a zatem wykonywanego w sposób zaprogramowany), nie występując jednocześnie przeciwko integralności zasobu, który w trakcie przenoszenia pomiędzy folderami zachowuje niezmienioną postać. Opisywany atak kierowany jest zatem wyłącznie przeciwko dostępności danych, która to cecha ujęta została wprost jedynie w pominiętej w przepisie przesłance. Jej brak, powoduje w efekcie realne osłabienie ochrony gwarantowanej przez art. 269 Kodeksu karnego.

Drugą z sygnalizowanych odrębności występujących pomiędzy konstrukcjami art. 268a oraz 269 Kodeksu karnego, jest natomiast usunięcie z redakcji art. 269 wymogu „istotności"[74] odnoszonego do stopnia penalizowanego zakłócenia automatycznego przetwarzania, gromadzenia lub przekazywania danych[75]. Wymóg taki, występujący na gruncie art. 268a, wyłącza karalność przypadków mniejszej wagi, w których zakłócenie pracy systemy nie narusza istotnych zasad jego funkcjonowania. Z uwagi na szczególny przedmiot ochrony przewidzianej w art. 269 - jakim są dane o szczególnym znaczeniu dla państwa, odnośna regulacja pozbawiona została wymogu „istotności", dzięki czemu wydatnie podwyższony został poziom ochrony danych „państwowych"[76], poprzez wprowadzenie penalizacji każdego przypadku zakłócenia ich automatycznego przetwarzania, gromadzenia lub przekazywania. Warto dodać, że przyjęta regulacja rozciąga się także na zakres penalizowanego usiłowania przeprowadzenia ataku na transmisję danych, obejmując próby wszelkich ataków, mogących potencjalnie zakłócić automatyczne przekazywanie danych o szczególnym znaczeniu dla obronności kraju lub funkcjonowania administracji państwowej.

Analizując opisywane przestępstwo cybernetyczne należy także wskazać, iż poruszane wyżej normy prawne art. 268a oraz 269 mogą pozostawać także w zbiegu z regulacją przepisu art. 165 § 1 pkt 4 Kodeksu karnego, w brzmieniu:

> „Art. 165 § 1 - 4). Kto, sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach: [pkt 4] zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekzywanie danych informatycznych – podlega karze pozbawienia wolności od 6 miesięcy do lat 8."

Przywołana jednostka redakcyjna wprowadziła penalizację czynu polegającego na „sprowadzeniu niebezpieczeństwa dla życia lub zdrowia" bądź też „mienia", dla których

---

[74] P. Kozłowska-Kalisz, op. cit., system LEX - komentarz do. art. 268a i 269.

[75] M. Siwicki, op. cit., s. 157.

[76] *Ibidem*, s. 157 oraz przywoływany tamże pogląd B. Kunickiej-Michalskiej, zawarty w: A. Wąsek, R. Zawłocki, Kodeks karny, Część szczególna, Komentarz do artykułów 222 – 316, t. II, Warszawa 2010, s. 736.

opisywane wcześniej przestępstwa stypizowane w art. 268a oraz 269 Kodeksu karnego stają się *de facto* środkiem sprawczym. Tym samym – w przypadku popełnienia czynu opisanego w przepisach art. 268a oraz 269 Kodeksu karnego w celu opisanym w art. 165 § 1 pkt 4 Kodeksu karnego, działanie takie może być kwalifikowane w zbiegu powyższych przepisów.

Czyn zabroniony określony w § 2 art. 269, odnoszący się do niszczenia danych przetwarzanych lokalnie, analizowany jest - zgodnie z przyjętym podziałem cyberprzestępstw, w części 4 rozdziału.

3. Zalewanie systemów nadmierną transmisją

Jak zostało zauważone na wstępie rozdziału, transmisja danych może występować w konstrukcji cyberprzestępstwa w dwojakiej roli - jako przedmiot ataku oraz jako narzędzie do jego popełnienia. Z tą drugą sytuacją mamy do czynienia w szczególności w przypadku przeprowadzania ataków typu *denial-of-service* (w skrócie, tzw. Dos) oraz *distributed-denial-of-service* (w skrócie nazywany Ddos), polegających na zakłócaniu realizacji usług świadczonych w sieci.

Każda usługa elektroniczna, która świadczona jest za pośrednictwem Internetu, opiera się *de facto* na przekazywaniu pomiędzy systemami teleinformatycznymi pakietów danych, ucieleśniających najróżniejsze, prawnie chronione dobra. Pośród dóbr tych wskazać należy w szczególności na dostępne poprzez strony WWW informacje i inne zasoby (np. grafiki, czy pliki muzyczne), zapisy systemów e-bankowych odzwierciedlające przepływające pieniądze i wreszcie najróżniejsze usługi, np. świadczenie poczty elektronicznej, czy też skanowanie komputera *on-line* w celu wykrycia ewentualnych wirusów komputerowych. Dla przeprowadzenia wymiany pakietów niezbędne jest nawiązanie połączenia pomiędzy systemami, którego zasady organizowania opisywano w rozdziale III pracy. W tym miejscu wypada jedynie przypomnieć, że każda transmisja danych składa się w rzeczywistości z dwóch elementów - jeden z systemów biorących udział w sieciowej wymianie danych musi dane te wysyłać, drugi zaś równolegle je odbierać. Zależność ta oznacza, że nie jest możliwe „jednostronne" pobranie jakiegokolwiek zasobu, bez czynnego udziału drugiego systemu, będącego drugą stroną komunikacji. Prezentując to zagadnienie na prostym przykładzie, zwyczajne otwarcie strony internetowej oznacza w praktyce wysłanie do serwera, na którym poszukiwana strona jest zlokalizowana, żądania, aby serwer zwrotnie wysłał do nas zawartość otwieranej witryny, w drugim kroku serwer realizuje to żądanie przekazując nam niezbędne dane za pośrednictwem sieci, zaś ostatecznie, nasz komputer odbiera transmitowane pliki oraz wyświetla ich treść użytkownikowi. W przykładzie tym pojawiają się dwa rodzaje połączenia

- pierwsze, żądanie strony (komputer domowy wysyła je do serwera) oraz drugie, transmitowanie strony (serwer wysyła pliki do komputera domowego). Co istotne, każde wysyłanie danych pozostaje skorelowane z ich automatycznym odbieraniem przez drugi system. Każda zaś z wymienionych operacji wymaga jednocześnie zaangażowania określonej mocy obliczeniowej komputerów oraz obciążenia dostępnego dla obydwu stron łącza internetowego.

Przedstawione zasady działania sieci wytworzyły możliwość wysyłania w bardzo krótkim czasie setek, czy nawet tysięcy zapytań o jedną stronę internetową, celem wymuszenia wzmożonej pracy atakowanego systemu oraz wydatne obciążenie jego łącza sieciowego. Przy całkowitym wykorzystaniu dostępnych zasobów sprzętowych oraz osiągnięciu limitu transferu danych, atakowana usługa staje się niedostępna dla innych użytkowników Internetu. Zdalne, umyślne wywołanie takiego przeciążenia otrzymało w języku komputerowym miano *ataku odmowy dostępu* (*denial-of-service*, Dos), która to nazwa odnosi się bezpośrednio do ograniczenia realizacji usług świadczonych przez zaatakowany system w jego normalnym stanie.

Ponieważ ręczne otwieranie zasobów internetowych jest zbyt wolne aby łatwo przeciążyć możliwości techniczne nowoczesnych serwerów oraz limity przepustowości dzisiejszych łączy internetowych, do przeprowadzania ataków Dos wykorzystuje się specjalnie przygotowane programy, zdolne do generowania tysięcy żądań na sekundę[77]. Proces wielokrotnego wysyłania niepotrzebnych zapytań nazywa się w żargonie informatycznym „zalewaniem" (z ang. *flooding*). Nawet w przypadku, gdy atakowany serwer posiada stosowne zabezpieczenia przed atakami typu Dos, samo odrzucanie wrogich żądań także zabiera określoną ilość mocy obliczeniowej. Tym samym, odpowiednio duża liczba zapytań jest w stanie zakłócić pracę każdego, nawet najwydajniejszego systemu teleinformatycznego, powodując albo czasowe zalanie systemu (stu procentowe wykorzystanie), albo jego awarię, wymagającą ponownego uruchomienia zaatakowanej usługi[78]. W skrajnych przypadkach przeciążony serwer może ulec fizycznemu uszkodzeniu.

Skuteczne atakowanie usług świadczonych przez duże serwisy internetowe opierające się na nowoczesnej, rozbudowanej infrastrukturze teleinformatycznej, wymaga preparowania tak dużych ilości zapytań, że ich przygotowanie oraz wysłanie nie jest możliwe przy wykorzystaniu pojedynczego systemu komputerowego. Współczesnym trendem

[77] Tak np. http://en.wikipedia.org/wiki/Denial-of-service_attack#Methods_of_attack.
[78] B. Hołyst, J. Pomykała, Cyberprzestępczość, ochrona informacji i kryptologia, Prokuratura i Prawo 2011, Nr 1, s. 9, przytaczam za: M. Siwicki, op. cit., s. 137.

w działalności cyberprzestępców stało się w efekcie przygotowywanie sieci komputerów - tzw. *botnetów*[79], które wykorzystywane są następnie do jednoczesnego atakowania obranych za cel systemów (*botnety* określa się czasami mianem „armii komputerów”). Przeprowadzony z ich wykorzystaniem atak nosi nazwę „rozproszonego ataku odmowy dostępu” (*distributed-denial-of-service*, Ddos), odwołującą się do faktycznej wielości źródeł ataku. Co istotne, użytkownicy komputerów wchodzących w skład przywołanych *botnetów*, najczęściej pozostają zupełnie nieświadomi faktu, że ich komputer jest lub może być wykorzystywany zdalnie przez cyberprzestępców (zwanych w tym wypadku *botmasters* lub też *botherders*[80]) do prowadzenia nieuprawnionych działań w sieci. Włączenie komputera do *botnetu* najczęściej odbywa się poprzez zainfekowanie go wirusem komputerowym lub wprowadzenie do niego innego oprogramowania złośliwego, przekształcającego komputer w tzw. *komputer zombie*. Wszelkie operacje wykonywane przez taki system w ramach nielegalnego działania *botnetu* są następnie skrzętnie ukrywane przez cyberprzestępców przed użytkownikami przejętych maszyn, manifestując się głównie w czasowo obniżonej wydajności komputera, czy też zmniejszonej przepustowości jego łącza.

Niezwykle interesującą odmianą ataku Ddos, jest także atak *distributed-reflected-denial-of-service* (Drdos)[81], polegający na zastosowaniu nieco bardziej wysublimowanego mechanizmu niż wysyłanie prostych żądań do atakowanego systemu. W trakcie ataku typu Drdos poszczególne komputery wykorzystywane do jego przeprowadzenia wysyłają do różnych systemów (innych niż atakowany) pakiety SYN, mające na celu nawiązanie połączenia internetowego pomiędzy zakończeniami sieci. Wysyłane pakiety posiadają sfałszowane adresy źródłowe IP (atak ten wykorzystuje zatem także opisywaną wcześniej technikę *IP-spoofing'u*), wskazujące adres systemu atakowanego. Poszczególne serwery, które otrzymały spreparowane pakiety SYN próbują następnie łączyć się ze wskazanym adresem IP, celem ustanowienia połączenia sieciowego, powodując przeciążenie wskazanego systemu-ofiary. Atak Drdos przeprowadzany jest w efekcie dwustopniowo, dodatkowo utrudniając prowadzenie czynności dowodowych mających na celu ustalenie rzeczywistego źródła cyberataku.

Przechodząc do analizy prawnej ataków typu Dos oraz Ddos, ich przeprowadzanie zostało spenalizowane na gruncie postanowień Konwencji o cyberprzestępczości w art. 5[82],

79 Więcej o botnetach na stronie internetowej pod adresem: http://us.norton.com/botnet/promo.
80 W tłumaczeniu, odpowiednio: „władcy botów” oraz „pasterze botów”. Tłumaczenie własne.
81 Tak np. http://en.wikipedia.org/wiki/Denial-of-service_attack#Reflected_.2F_Spoofed_attack.
82 Przepis ten zatytułowany został „Zakłócenie systemu”. W oryginale „*System interference*”. Tłumaczenie własne. W oficjalnym tłumaczeniu Konwencji przytoczony zwrot przetłumaczono jako „Naruszenie

przyjmującym brzmienie:

> „Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego, popełnionego umyślnie czynu polegającego na istotnym, bezprawnym zakłócaniu funkcjonowania systemu komputerowego poprzez wprowadzanie, transmisję, niszczenie, usuwanie, uszkadzanie, modyfikowanie lub utrudnianie dostępu do danych komputerowych”[83].

Zawarty w Konwencji budapesztańskiej przepis penalizuje szereg cyberataków polegających na zakłócaniu poprawnego funkcjonowania systemów, pośród których wymienić należy także ataki typu Dos oraz Ddos. Warto nadmienić, że oryginalna nazwa ataku - *denial-of-service*, została wyraźnie przewidziana w pkt 67 Raportu wyjaśniającego do Konwencji, komentującego właśnie art. 5. Pomimo szerokiego zakresu przedmiotowego przepisu, zawarta w tym miejscu analiza art. 5 Konwencji, została ograniczona do przybliżenia regulacji karnej odnoszącej się do ataków typu Dos oraz Ddos.

Zgodnie z przyjętym brzmieniem przepisu art. 5 Konwencji, jako przestępne zidentyfikowane zostało działanie polegające na umyślnym, bezprawnym oraz istotnym zakłóceniu funkcjonowania systemu komputerowego, dokonywane między innymi poprzez transmisję danych komputerowych lub też utrudnianie dostępu do tych danych. W przypadku dokonywania kwalifikacji prawnej ataków typu Dos oraz Ddos, przesłanki te należy traktować łącznie. W atakach tych, transmisja danych wykorzystywana jest w roli narzędzia sprawczego, stanowiąc niezbędny element *modus operandi* sprawcy charakteryzowanych cyberataków. Następnie, nadmierna transmisja danych - „zalewająca” atakowany system, wywołuje zakłócenia w jego pracy, które manifestują się w szczególności, utrudnieniami w dostępie do danych, które przetwarzane są przez system. Tym samym, każdy skutecznie przeprowadzony atak typu Dos lub Ddos, wypełnia w istocie dwie równorzędne przesłanki uznania za cyberprzestępstwo określone w art. 5 Konwencji. Utrudnienie dostępu do danych jest bowiem w tym wypadku powodowane bezprawnym wykorzystaniem transmisji danych, traktowanej przez cyberprzestępcę jako narzędzie ataku.

Na tle powyższych rozważań zasadne wydaje się postawienie pytania - w którym

---

integralności systemu”.

[83] W oryginale: „*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*”. Tłumaczenie własne. W oficjalnym tłumaczeniu Konwencji wymieniony w przepisie katalog czynności przestępnych został ujęty, jako „wprowadzanie, transmisja, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie”.

momencie, zwykła transmisja danych, polegającą na standardowym otwieraniu dostępnych publicznie stron internetowych, staje się bezprawna? Co było podkreślane w części poświęconej *quasi*-technicznemu opisowi ataków typ Dos oraz Ddos, ataki te często polegają na zwykłym wywoływaniu witryn internetowych, tyle, że dokonywanym z nienaturalną częstotliwością. Ile zatem razy trzeba dokonać żądania otwarcia określonej strony, aby działanie takie móc uznać za bezprawne? Także, czy pojedyncze otwarcie strony, powodujące jednak przepełnienie już mocno obciążonego łącza, może być uznane za działanie przestępne? Pomimo pozornej trywialności powyższych pytań, przedstawiona kwestia na razie nie doczekała się jednoznacznego uregulowania prawnego. Dokumenty takie jak Konwencja o cyberprzestępczości, czy też Decyzja Ramowa Rady Unii Europejskiej w sprawie ataków na systemy informatyczne oraz zastępująca ją Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne[84], pozostawiają opisywany problem prawodawstwom krajowym nie mogąc znaleźć satysfakcjonującego kompromisu, który wyznaczałby prawną granicę ataków odmowy dostępu. W doktrynie prawnej, gdy analizuje się ataki typu Dos lub Ddos, niejako automatycznie rozumie się przez to przypadki ewidentne, w których system atakujący (w tym też zainfekowany komputer *zombie* należący do *botnetu*) wykonuje na sekundę setki prób otwarcia jednej strony internetowej lub też odwołań do jednej, określonej usługi sieciowej. Działania takie pozostają w sposób oczywisty sprzeczne z typowymi potrzebami użytkownika sieci, łamiąc jednocześnie przyjęte w cyberprzestrzeni - choć niespisane, konwenanse. W praktyce tego typu operacje przyjęło się nazywać „bezprawnymi". Obok jednoznacznych przypadków atakowania systemów teleinformatycznych istnieją jednak także sytuacje kontrowersyjne, w których bezprawność działań użytkowników cyberprzestrzeni nie poddaje się prostej ocenie. Przykładowo - w sieci dostępnych jest wiele darmowych usług, np. wykonujących tłumaczenia językowe *on-line*[85]. Usługi te realizowane są najczęściej za pośrednictwem interfejsu umieszczonego bezpośrednio na stronie internetowej. Interfejs taki może zostać wykorzystany do tłumaczenia bądź pojedynczych słów, bądź też całych stron tekstu. Zadać można więc pytanie - czy wprowadzenie do tłumaczenia w takim interfejsie wielostronicowego dokumentu, mogące potencjalnie zawiesić na pewien czas dostępność usługi dla innych użytkowników (a zatem wywołać skutek analogiczny do ataku Dos), może zostać uznane za formę ataku? Poszukując rozwiązań prawnych, które mogłyby stanowić

[84] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

[85] Przykładowo wskazać można serwis *Google Translate*, dostępny na stronie internetowej pod adresem: http://translate.google.pl/.

w tym miejscu wskazówkę interpretacyjną, warto odwołać się do postanowień pierwotnych Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, na gruncie której przewidziano wprost definicję „bezprawności", rozumiejąc pod tym pojęciem:

> „[...] dostęp lub ingerencję, na którą właściciel, inny posiadacz prawa do systemu lub jego części nie udzielił zgody lub która nie jest dozwolona na mocy prawa krajowego."[86],

- oraz analogicznych rozwiązań na gruncie Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne[87], która zastępując przywołaną Decyzję, stanowi w sposób zbieżny, iż:

> „„bezprawnie" oznacza działanie, o którym mowa w niniejszej dyrektywie, w tym dostęp, ingerencje lub przechwycenie, na które właściciel lub inny uprawniony do systemu lub jego części nie udzielił zgody, lub które nie jest dozwolone na mocy prawa krajowego."

Tym samym, bezprawność transmisji danych - która to transmisja, co do zasady stanowi przecież legalny sposób wymiany danych oraz informacji, w przypadku braku jednoznacznych regulacji krajowych, powinna być oceniana przez organy procesowe *ad casum* z uwzględnieniem panujących w cyberprzestrzeni zwyczajów, rozwiązań technologicznych, a także zasad pracy danego systemu. Na tle tego ostatniego wymogu rysuje się jednak istotna wada praktyczna proponowanego rozwiązania - zdecydowana większość usług sieciowych nie wymaga ani zapoznawania się, ani tym bardziej akceptowania żadnych regulaminów świadczenia usług. Co ciekawe, Raport Wyjaśniający do Konwencji o cyberprzestrzeni - która to Konwencja w odróżnieniu od postanowień Decyzji Ramowej nie definiuje „bezprawności" działań, zwraca uwagę na kategorię działań „prawnych", które mogąc powodować zmiany w pracy określonego systemu teleinformatycznego, nie podlegają kwalifikacji, jako działania „bezprawne". Pośród tego typu operacji w Raporcie wskazane zostały testy bezpieczeństwa wykonywane na zlecenie właściciela systemu, czy też dobrowolne instalowanie nowego oprogramowania, które w procesie instalacji usuwa z komputera starsze wersje programów lub wprowadza do nich istotne zmiany. Takie działania nie podlegają penalizacji, choć w sposób istotny wpływają na pracę systemu (obrazowo można w tym miejscu powiedzieć o zamierzonych przez użytkownika

[86] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW.

[87] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

zakłóceniach pierwotnej pracy systemu)[88]. Ocena ta pozostaje w pełnej zgodności z przytoczoną wyżej za Decyzją Ramową definicją pojęcia „bezprawności".

Zgodnie z postanowieniem art. 5 Konwencji zakłócenie pracy systemu musi ponadto być „istotne" ażeby móc uznawać je za działanie przestępne. O ile w tekście Konwencji przesłanka ta pozostawiona została bez żadnego wyjaśnienia, o tyle pewne przybliżenie jej treści można odnaleźć ponownie w Raporcie Wyjaśniającym. W pierwszej kolejności, jakstanowi pkt 67 Raportu, kryterium „istotności" powinno zostać dookreślone przez każde z państw-stron konwencji indywidualnie w przepisach krajowych. Jako wskazówkę legislacyjną, autorzy Raportu zaznaczyli w tym miejscu możliwość odniesienia wymaganej przesłanki do określonego rozmiaru szkód wyrządzonych bezprawnym działaniem w cyberprzestrzeni. Niejako na drugi plan zsunięta została natomiast propozycja innego rozwiązania prawnego, stanowiąca że za istotne zakłócenie pracy systemu spowodowane wysyłaniem danych, autorzy Raportu uznają działanie podejmowane w takiej formie, rozmiarze lub częstotliwości, które wywiera znaczący, szkodliwy wpływ na możliwości korzystania z usług świadczonych przez system, w tym jego zdolność komunikacji z innymi systemami teleinformatycznymi[89]. Komentując powyższe propozycje można zauważyć, że o ile pierwsze rozwiązanie wydaje się być nietrafione z uwagi na wprowadzanie miary wielkości ataku, która odwołuje się do wartości ekonomicznych zamiast oceny samego ataku, o tyle druga propozycja, choć słusznie nakierowana na badanie zakłóceń w pracy atakowanego systemu, w dalszym ciągu posługuje się wysoce ocennymi określeniami, jak „znaczący, szkodliwy wpływ", przekreślającymi jej wymiar praktyczny. W rezultacie, ocena „istotności" ataku pozostawiona została do wyłącznej gestii prawodawców krajowych.

Ograniczając prowadzoną w tym miejscu analizę do oceny prawnej ataków dokonywanych w ramach transmisji danych, analogiczną budowę do rozwiązań przyjętych w Konwencji o cyberprzestępczości przyjęła także regulacja penalizująca ataki typu Dos oraz

---

[88] W oryginale: „*The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorised by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalised by this article, even if it causes serious hindering.* ".

[89] Pkt 67 Raportu. W oryginale: „*The hindering must furthermore be "serious" in order to give rise to criminal sanction. Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).* ".

Ddos, która wprowadzona została na gruncie Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[90] oraz następnie przeniesiona do Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne. Zgodnie z art. 3 Decyzji:

> „Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślne poważne naruszenie lub przerwanie funkcjonowania systemu informatycznego poprzez wprowadzanie, przekazywanie, uszkadzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych jest karalne jako przestępstwo, kiedy dokonane jest bezprawnie, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.”.

Zgodnie zaś z art. 4 Dyrektywy:

> „Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne i bezprawne poważne utrudnienie lub zakłócenie funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych lub czynienie ich niedostępnymi, było karalne jako przestępstwo, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.”

Zawężając zakres interpretacji przytoczonych przepisów do normy sankcjonującej ataki typu Dos oraz Ddos, tak jak w przypadku postanowień Konwencji o cyberprzestępczości, przesłankami karalności tak określonych czynów są:

1) umyślność działania sprawcy cyberataku;
2) bezprawność ataku;
3) przeprowadzenie ataku poprzez przekazywanie danych lub uczynienie danych niedostępnymi - skorelowane w przypadku ataków Dos oraz Ddos, o czym pisano powyżej; oraz,
4) odpowiedni poziom naruszenia funkcjonowania atakowanego systemu („poważne naruszenie lub przerwanie funkcjonowania systemu), z ewentualnym wyłączeniem przypadków mniejszej wagi.

Z uwagi na zbieżność analizowanych regulacji, przyjętych na gruncie Konwencji Budapesztańskiej oraz w Decyzji Ramowej Rady Unii Europejskiej, wcześniejsze uwagi poczynione wobec postanowień Konwencji o cyberprzestępczości, ponownie zachowują

---

[90] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW.

swoją pełną aktualność także w odniesieniu do przepisu Decyzji Ramowej, przez co nie będą powtarzane. Warto w tym jednak miejscu ponownie podkreślić, że w postanowieniach Decyzji Ramowej pojawia się (również przeanalizowana wyżej) definicja pojęcia „bezprawności", przybliżająca rzeczywiste znaczenie ataków Dos oraz Ddos. Odnośnie zaś pojawiających się różnic językowych w tłumaczeniu znamienia „zatajania / eliminacji" – *vide* wcześniejsze uwagi, poczynione w tym zakresie na gruncie rozważań dot. nielegalnego przechwytywania transmisji danych.

Wskazując na krajowe regulacje karne sankcjonujące przeprowadzanie ataków typu Dos oraz Ddos, przywołać należy aż cztery przepisy Kodeksu karnego, zawarte w art. 268 - 269a:

> „Art. 268. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
>
> § 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
>
> § 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
>
> § 4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.
>
> Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.
>
> § 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
>
> § 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.
>
> Art. 269. § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
>
> § 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo

wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a. Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.".

W oparciu o wybrane fragmenty powyższych przepisów zbudować można następującą normę prawną sankcjonującą ataki typu Dos oraz Ddos[91]:

- kto udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z informacją, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. O ile czyn dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. W przypadku wyrządzenia znacznej szkody majątkowej - do lat 5. Ściganie następuje na wniosek pokrzywdzonego (art. 268 Kk),
- kto utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3. Sankcja wzrasta do lat 5 w przypadku wyrządzenia czynem znacznej szkody majątkowej. Czyn (tak jak poprzednio) ścigany jest na wniosek pokrzywdzonego (art. 268a Kk),
- kto zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Czyn ścigany jest z urzędu (art. 269 Kk),
- kto przez transmisję lub utrudnienie dostępu do danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 5. Czyn ścigany jest z urzędu (art. 269a Kk).

Z powyższego zestawienia wyłania się rozbudowana norma prawna odnosząca się do ataków odmowy dostępu, której struktura niepozbawiona jednak kilku istotnych niespójności. Po pierwsze, brak jest jednoznacznego kryterium, które w przypadku kwalifikacji prawnej

[91] P. Kozłowska-Kalisz, op. cit., system LEX - komentarz do art. 268 - 269a k.k. oraz W. Wróbel, op. cit., system LEX - komentarz do art. 268 - 269a k.k., A. Lach, op. cit., system LEX - komentarz do art. 267 k.k.

ataków typu Dos oraz Ddos (ale także i innych ataków), uzasadniałoby rozdział przepisów art. 268, 268a oraz 269a Kodeksu karnego[92]. Przepisy art. 268 oraz 268a zróżnicowane zostały *de facto* w oparciu o przeciwstawienie czynów skierowanych przeciwko informacjom oraz czynów skierowanych przeciwko danym. Co było podkreślane także wcześniej, rozróżnienie to jest sztuczne, jako że w systemach komputerowych wszelkie informacje budowane są z danych zapisywanych na informatycznych nośnikach. Innymi słowy, przeprowadzając cyberatak nie jest możliwe wpływanie na same dane lub też same informacje - bowiem obie te kategorie są ze sobą ściśle, wręcz *genetycznie*, powiązane. Po drugie, dla dalszego skomplikowania sytuacji, art. 269a Kk sankcjonuje czyn polegający na zakłóceniu pracy systemu komputerowego lub sieci komputerowej, wprowadzając tym samym ujęte synonimicznie, choć inaczej zredagowane, znamiona czynu bezprawnego w porównaniu do tych znanych z art. 268 oraz 268a Kk: „udaremniania lub znacznego utrudniania zapoznania z informacją" oraz „zakłócania automatycznego przetwarzania danych". W istocie uznać należy, że zakłócanie lub utrudnianie automatycznego przetwarzania danych stanowi jednocześnie zakłócenie pracy systemu komputerowego lub też sieci (w tym drugim wypadku o ile tylko zakłócane są operacje wykonywane przez serwery obsługujące łączność sieciową). Zależność ta działa także w przeciwnym kierunku - zakłócenie pracy systemu zawsze wiązać się będzie z zakłócaniem automatycznego przetwarzania danych (można powiedzieć, że wszystkie operacje wykonywane przez komputery polegają na szeroko rozumianym przetwarzaniu danych). I wreszcie po trzecie – o ile przestępstwa stypizowane w art. 268 oraz 268a Kk ścigane są na wniosek pokrzywdzonego, o tyle przestępstwo z art. 269a Kk ścigane jest z urzędu - pomimo, że zarówno art. 268 Kk, jak również art. 268a Kk dotyczą także przypadków kwantyfikowanych, jako „istotne" lub „znaczne". Na tle regulacji art. 268, 268a oraz 269a Kk w sposób jasno wyodrębniony został jedynie przepis art. 269 Kk regulujący szczególne przypadki ataków cybernetycznych, które kierowane są przeciwko systemom istotnym z punktu widzenia funkcjonowania oraz bezpieczeństwa państwa[93].

Przechodząc do bliższej analizy poszczególnych jednostek redakcyjnych pod kątem ich zastosowania do zwalczania ataków odmowy dostępu, należy wskazać na następujące

[92] Kwestia nakładania się zakresów przedmiotowych wymienionych przepisów poruszana była w doktrynie m.in. przez prof. A. Adamskiego. Tak np. w: Cyberprzestępczość..., op. cit., s. 58. Tak również: W. Wróbel, op. cit., system LEX - komentarz do art. 268a - 269k.k.

[93] A. Sakowicz, Kodeks karny - część szczególna, tom 2, pod red. M. Królikowski, R. Zawłocki, Warszawa 2013, s. 453.

cechy komentowanych regulacji. Odnośnie art. 268 Kodeksu karnego[94]:

- zgodnie z literalnym brzmieniem art. 268 § 1 Kk, na gruncie przepisu penalizowane jest znaczne utrudnianie lub też całkowite udaremnienie osobie uprawnionej zapoznania się istotną informacją. Tym samym, utrudnianie w sieci innych czynności niż „zapoznawanie" pozostawione zostało poza zakresem regulacyjnym przepisu, np. utrudnianie modyfikacji, czy też uniemożliwianie usunięcia informacji, niestanowiące przecież w żadnym razie desygnatów pojęcia „zapoznanie". Warto w tym miejscu przypomnieć, że od strony technicznej, atak odmowy dostępu obejmuje każde ograniczenie usług lub czynności dostępnych dla użytkownika, zarówno tych realizowanych na jego rzecz, jak i wykonywanych samodzielnie,
- zakres ochrony oferowanej przez przepis ograniczony został do przypadków kwantyfikowanych dwiema wartościami ocennymi - po pierwsze, utrudnienie musi być „znaczne", po drugie zaś, informacja, której utrudnienie dotyczy, musi być „informacją istotną"[95]. Pojęcia te nie są niestety w żadnej mierze przybliżane na gruncie ustawy. W doktrynie podkreśla się, że ocena „istotności" informacji dokonywana winna być zawsze w odniesieniu do konkretnych okoliczności w ujęciach subiektywnym oraz obiektywnym[96], z uwzględnieniem znaczenia informacji dla jej dysponenta oraz atakującego[97]. Negatywną implikacją przyjętej regulacji jest wyłączenie karalności nawet skomplikowanego ataku, o ile tylko jego zasięg nie objął informacji, które jednoznacznie należy uznawać za istotne. Jeszcze więcej problemów nastręcza ustalenie, kiedy utrudnienie dostępu uznawać należy za „znaczne". Ponownie, zastosowanie znajdować muszą tu kryteria zarówno subiektywne, jak i obiektywne, jako że dla jednej osoby opóźnienie pracy serwera wynoszące dwie sekundy (tu z odwołaniem do miary czasu[98]) może być nie-znaczne, jednak dla ogromnej serwerowni obsługującej miliony połączeń - zupełnie nie akceptowalne. Oba wprowadzone kwantyfikatory stanowią w ocenie Autora niniejszej pracy nieudaną - zarówno merytorycznie, jak i legislacyjnie, próbę wyłączenia

---

[94] P. Kozłowska-Kalisz, op. cit., system LEX - komentarz do art. 268 k.k.

[95] W. Wróbel, op. cit., system LEX - komentarz do art. 268 k.k., A. Lach, op. cit., system LEX - komentarz do art. 268 k.k., J. Giezek, Kodeks karny. Część szczególna. Komentarz, pod red. J. Giezek, D. Gruszecka, N. Kłączyńska, G. Łabuda, A. Muszyńska, T. Razowski, LEX 2014, system LEX - komentarz do art. 268. k.k.

[96] J. Piórkowska-Flieger op. cit., s. 593.

[97] M. Kalitowski op. cit., s. 1146.

[98] Kryterium czasu, jako jedno z możliwych do zastosowania przywołane jest przez J. Piórkowska-Flieger, op. cit., s. 593.

odpowiedzialności karnej w przypadkach mniejszej wagi. Przyjęta redakcja w szczególności nie spełnia standardów przejrzystości prawa,

- utrudnianie dostępu do informacji może być dokonywane poprzez zaburzanie wielu różnych rodzajów usług - typowymi przykładami są tu: zakłócanie dostępności strony WWW, zakłócanie możliwości wysłania lub odbioru poczty e-mail, czy też przeprowadzanie ataków odmowy dostępu przeciwko samej zdolności atakowanego systemu do transmisji danych,
- co wynika wprost z § 2 analizowanego art. 268 Kk, w przypadku, gdy opisywany w tym przepisie czyn dotyczy „zapisu na informatycznym nośniku danych", sprawca może zostać ukarany karą surowszą, to jest karą 3 lat pozbawienie wolności, w opozycji do podstawowego typu zagrożonego karą 2 lat. Ponieważ wszelkie dane komputerowe - w tym programy, strony internetowe oraz wszelkie zasoby audio-wizualne, składowane są zawsze na szeroko rozumianych informatycznych nośnikach danych, należy przyjąć, że każdy atak typu Dos oraz Ddos powodować będzie ograniczenia w dostępności usług, które odwołują się do cyfrowego zapisu danych przechowywanych na takich nośnikach. Jako najprostszy przykład tej zależności wskazać należy na zaprezentowane szerzej w rozdziale III zasady funkcjonowania stron internetowych - każda strona WWW stanowi w istocie zbiór plików zapisanych w pamięci serwera zapewniającego *hosting* danej witryny. W efekcie, każdy atak Dos oraz Ddos *dotyka* danych zapisanych na informatycznym nośniku danych, wypełniając jednocześnie znamiona obydwu typów przestępstwa stypizowanego w art. 268 Kk - to jest podstawowego (§ 1) oraz kwalifikowanego (§ 2).

Odnośnie art. 268a Kodeksu karnego warto wskazać, że:

- w odniesieniu do penalizacji ataków Dos oraz Ddos, komentowany przepis sankcjonuje nie tylko utrudnienie dostępu do danych, ale także zakłócanie automatycznego przetwarzania danych, co w stosunku do regulacji art. 268 Kk, stanowi istotne rozszerzenie zakresu przedmiotowego przepisu[99]. W oparciu o art. 268a Kk możliwe jest w efekcie ściganie nie tylko ataków Dos oraz Ddos wpływających na możliwość „otwarcia" danego zasobu (*vide* przesłanka „utrudniania zapoznania się z informacją" z art. 268 Kk), ale także ataków skierowanych na uniemożliwienie użytkownikowi realizacji innych działań, jak np. usunięcia, czy modyfikacji określonego zasobu,

[99] P. Kozłowska-Kalisz, op. cit., system LEX - komentarz do art. 268 a k.k.

- analizowany przepis penalizuje utrudnianie dostępu do wszelkich danych informatycznych, nie ograniczając swojego zakresu ochrony do danych „istotnych”, jak czynił to przepis art. 268 Kk. Tym samym, podczas stosowania normy art. 268a Kk nie ma potrzeby przeprowadzania badania „jakości” danych, które stały się przedmiotem ataku[100]. W dalszym ciągu pozostawione jednak zostało znamię „istotnego stopnia zakłócenia” automatycznego przetwarzania danych,
- ponieważ przepis nie odwołuje się ani do określonych kategorii danych informatycznych, ani rodzajów atakowanych usług, jego zakres przedmiotowy obejmuje wszelkie dane: w szczególności pliki składające się na strony WWW, wiadomości e-mail, wszelkie wpisy na forach, hasła (w tym zaszyfrowane) oraz materiały audio-wizualne. Bez znaczenia pozostaje również fakt, czy atakowane są dane przechowywane na trwałym nośniku, przetwarzane w ulotnej pamięci, czy też podróżujące przez sieci,
- pomimo objęcia przepisem także najpoważniejszych, rozległych ataków Dos oraz Ddos, które potencjalnie kierowane mogą być przeciwko istotnym usługom świadczonym na rzecz obywateli, np. usługi e-bankowe, w tym ataków wywołujących znaczną szkodę majątkową (§ 2), przestępstwo stypizowane w art. 268a Kk ścigane jest na wniosek pokrzywdzonego. Rozwiązanie takie należy oceniać, jako ograniczające ochronę interesów osób, które korzystają z atakowanej usługi, nie są zaś jej oferentami. W praktyce, złożenie wniosku o ściganie pozostawione jest często do wyłącznej gestii administratora atakowanej usługi, który nie chcąc ujawnić swoich niedociągnięć w odniesieniu do zapewnienia bezpieczeństwa systemu, może odstąpić od złożenia wniosku, a tym samym wszczęcia procesu karnego. Problem identyfikacji pokrzywdzonych atakami typu Dos oraz Ddos przybliżony został szerzej po uwagach szczegółowych do art. 268 - 269a Kk.

Odnośnie art. 269 Kodeksu karnego warto zauważyć, że:

- jako *lex specialis* wobec regulacji art. 268a Kk, przedmiotowy przepis wprowadza szczególną ochronę systemów oraz danych ważnych z punktu widzenia bezpieczeństwa oraz funkcjonowania państwa[101]. W szczególności, uznać należy, że art. 269 Kk obejmuje swoją ochroną teleinformatyczne elementy infrastruktury

[100] *Ibidem.*
[101] W. Wróbel, op. cit., LEX 2013, system LEX - komentarz do art. 269 k.k.

krytycznej, definiowanej w przepisach ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[102],

- z uwagi na szczególny przedmiot ochrony, na gruncie przepisu 269 Kk nie jest wymagane aby atakowane dany były „istotne” (badane jest wyłącznie spełnienie obiektywnego kryterium rodzaju danych), jak również to, ażeby zakłócenie ich automatycznego przetwarzania nosiło znamię „znaczności”. Komentowany przepis odnosi się tym samym wszelkich przypadków - w tym także przypadków mniejszej wagi, w których tylko celem ataku są, ogólnie ujmując, dane oraz systemy wrażliwe dla funkcjonowania państwa,
- w związku z analogiczną budową przepisów art. 268a oraz 269 Kk, zasadne mogłoby się wydawać, aby lista znamion czynów bezprawnych opisywanych w tych przepisach była zbieżna lub rozszerzona na rzecz przepisu szczególnego, zapewniającego ochronę systemom kluczowym dla funkcjonowania całego państwa. Porównując jednak zakresy przesłanek określonych w art. 269 Kk oraz 268a Kk, zauważyć można, że w komentowanej jednostce redakcyjnej brak jest odwołania do znamienia „utrudniania dostępu” do danych, co stanowi zawężenie zakresu przedmiotowego przepisu. Tym samym, na gruncie art. 269 Kk do zwalczania ataków typu Dos oraz Ddos odwołuje się jedynie ogólna przesłanka, stanowiąca o „zakłócaniu lub uniemożliwianiu automatycznego przetwarzania danych”. Zgodnie jednak z wcześniejszymi uwagami, należy uznać, że każdy przypadek utrudniania dostępu do danych, stanowi jednocześnie przynajmniej zakłócanie (o ile nie uniemożliwianie) procesu ich automatycznego przetwarzania. Z uwagi jednak na szczególny przedmiot ochrony, różnicowanie przesłanek określonych w art. 268a oraz 269 Kk w sposób okrawający ochronę systemów państwowych, wydaje się być działaniem ryzykownym, dopuszczającym interpretację o zamierzonym przez ustawodawcę zabiegu legislacyjnym. Zgodnie z metodyką interpretacji językowej, dwóm różnym przepisom należy przecież przypisywać dwa różna znaczenia,
- z racji szczególnego przedmiotu ochrony, przestępstwa stypizowane w art. 269 Kk podlegają ściganiu z urzędu.

Ostatecznie, odnośnie art. 269a Kodeksu karnego[103]:

[102] Dz. U. z 2007 r. Nr 89, poz. 590, z późn. zm.
[103] A. Lach, op. cit., system LEX - komentarz do art. 269a k.k., J. Giezek, op. cit., system LEX - komentarz do art. 269a. k.k.

- art. 269a Kk jest jedynym przepisem, do którego ustawodawca zdecydował się wprowadzić przesłankę „zakłócania pracy systemu komputerowego lub sieci teleinformatycznej”, zastępując nią znaną z poprzedzających jednostek redakcyjnych przesłankę „zakłócania automatycznego przetwarzania danych”. Przedstawiona odrębność niesie ze sobą dwie istotne, wskazane poniżej implikacje,
- po pierwsze, zastosowane sformułowanie nakazuje odnosić normę prawną art. 269a Kk do ochrony pracy dwóch określonych (nazwanych) rozwiązań technicznych: systemu komputerowego oraz sieci teleinformatycznej. W efekcie przyjętego nazewnictwa, dla określenia faktycznego zasięgu regulacyjnego analizowanej normy, niezbędne staje się uprzednie wyznaczenie desygnatów przytoczonych pojęć „system komputerowy” oraz „sieć teleinformatyczna”. Ponieważ obydwa pojęcia nie posiadają swoich definicji legalnych (choćby typologicznych), ich znaczenie musi być rekonstruowane w oparciu o powszechne rozumienie zastosowanych wyrażeń. Przez „system komputerowy” należy zatem rozumieć w szczególności komputery klasy PC (zarówno stacjonarne jak i przenośne) oraz ich elementy - słowo „system” sugeruje zbiór podzespołów. Do „sieci teleinformatycznych” zaliczyć trzeba natomiast całą infrastrukturę sieciową, w szczególności serwery, jak również wszelkie urządzenia kierujące ruchem oraz zestawianiem łączy. Poza możliwością dokonania jednoznacznej kwalifikacji pozostają urządzenia takie, jak nowoczesne *smartfony*, czy tablety z modemem 3G, będące w istocie hybrydami urządzeń komputerowych oraz telefonów komórkowych, a także wysoce specjalistyczne systemy produkcyjne (np. roboty w fabryce samochodów) i wreszcie systemy SCADA[104] (systemy obsługujące np. elektrownie atomowe, przepompownie wody, tamy, itd). Ocena ich przynależności do desygnatów pojęcia „system komputerowy” będzie zatem musiała być dokonywana w ramach konkretnych przypadków, z zastosowaniem kryteriów subiektywnych (związanych z całokształtem okoliczności sprawy), jak również obiektywnych (związanych m.in. z aktualnym stanem rozwoju techniki). Abstrahując od samej definicji „systemu komputerowego” warto zauważyć, że wszelkie ataki kierowane przeciwko urządzeniom połączonym w sieci, w tym choćby sieci lokalne, mogą być zaliczane do ataków przeciwko sieciom teleinformatycznym, wykluczając tym samym konieczność dokonywania oceny, czy zaatakowane urządzenia to systemy komputerowe, czy też nie,

[104] Anglojęzyczny skrót SCADA rozwija się jako *supervisory control and data acquisition*. W wolnym tłumaczeniu: „Systemy kontroli oraz pozyskiwania danych”. Tłumaczenie własne.

- przechodząc do kwestii drugiej - związanej z ochroną *pracy* systemów i sieci, należy uznać, że zastosowane w przepisie wyrażenie „praca” jest semantycznie szersze od wyrażenia „automatyczne przetwarzanie danych”. O ile przetwarzanie danych z pewnością stanowi pracę systemów, o tyle nowoczesne urządzenia komputerowe mogą wykonywać także zadania fizyczne, jak np. sygnalizowane wyżej systemy SCADA. Wykonywana przez nie praca może polegać np. otwieraniu zbiorników retencyjnych, czy zamykaniu tam, a więc *dokonywaniem faktycznych zmian w realnym świecie* (wyjście poza cyberprzestrzeń). Niemniej, wszelkie te działania, na najniższym poziomie funkcjonowania systemów komputerowych opierają się *de facto* na przetwarzaniu danych (np. włączenie siłownika poprzedzone musi być przetworzeniem stosownej komendy), a zatem każde zakłócenie pracy urządzenia wywołane poprzez atak cybernetyczny będzie wiązać się z uprzednim zakłóceniem zaplanowanego, poprawnego przetwarzania danych w atakowanym urządzeniu,
- analizując przepis art. 269a Kk wyłącznie pod kątem penalizacji ataków typu Dos oraz Ddos, należy stwierdzić, że do ataków tych odnoszą się dwa spośród sześciu wprowadzonych do redakcji przepisu znamion popełnienia przestępstwa, tj.: „poprzez transmisję” oraz „poprzez utrudnienie dostępu”. De facto każdy atak typu Dos oraz Ddos wypełnia oba wskazane znamiona jednocześnie, co wynika bezpośrednio z jego charakterystyki technicznej. Warto podkreślić, że w przypadku ataków Dos oraz Ddos znamię „utrudnienia dostępu” oraz zapisany w przepisie skutek przestępstwa - „zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej”, pozostają w istocie zbieżne. Owo utrudnienie dostępu nie wywołuje bowiem zakłócenia, lecz samo w sobie stanowi to zakłócenie,
- ostatecznie, dla ścigania ataków typu Dos lub Ddos na gruncie art. 269a Kk, zakłócenie pracy systemu (czyli utrudnienie dostępu do niego), musi być kwantyfikowane, jako istotne w stopniu (vide wcześniejsze uwagi do regulacji art. 268 oraz 268a Kk).

Podobnie, jak było wskazywane w poprzedniej części rozdziału, także w przypadku przestępstwa zalewania systemów nadmierną transmisją danych może dochodzić do zbiegu opisywanych wyżej przepisów z normą prawną art. 165 § 1 pkt 4 Kodeksu karnego, w brzmieniu:

„Art. 165 § 1 - 4). Kto, sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach: [pkt 4] zakłócając, uniemożliwiając lub w inny

sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych – podlega karze pozbawienia wolności od 6 miesięcy do lat 8.”

Przywołana jednostka redakcyjna typizuje czyn polegający na „sprowadzeniu niebezpieczeństwa dla życia lub zdrowia” bądź też „mienia”, dla których opisywane wyżej przestępstwa mogą stać się środkiem sprawczym. Tym samym – w przypadku popełnienia czynu opisanego w przepisach art. 268-269a Kodeksu karnego w celu opisanym w art. 165 § 1 pkt 4 Kodeksu karnego, działanie takie może być kwalifikowane w zbiegu powyższych przepisów.

Na zakończenie analizy prawnej penalizacji ataków odmowy dostępu, za konieczne należy uznać poruszenie kwestii o szczególnej doniosłości procesowej, związanej z możliwością wystąpienia bardzo dużej liczby osób pokrzywdzonych w sensie formalnym, pojedynczym atakiem typu Dos lub Ddos. Ponieważ skuteczny atak odmowy dostępu kierowany np. przeciwko serwerom pocztowym określonego usługodawcy (np. poczta Onetu, czy Wirtualnej Polski), powoduje niedostępność poczty elektronicznej dla całej grupy użytkowników określonej usługi, zasadnym staje się postawienie pytania o sposób wyznaczania kręgu pokrzywdzonych takim przestępstwem. Kwestia ta posiada istotne znaczenie procesowe już od samego początku postępowania, m.in. wskazując osoby uprawnione do złożenia wniosku o ściganie przestępstwa z art. 268 oraz 268a Kk. Zgodnie z art. 49 § 1 Kodeksu postępowania karnego:

„Pokrzywdzonym jest osoba fizyczna lub prawna, której dobro prawne zostało bezpośrednio naruszone lub zagrożone przez przestępstwo.”.

Odwołując się do przytoczonego wyżej przykładu ataku na serwery poczty elektronicznej, z przepisu art. 49 Kpk wynika, że pokrzywdzonym tego typu atakiem, jest co najmniej każdy zarejestrowany użytkownik zaatakowanej usługi pocztowej, który nie mógł skorzystać ze świadczonych na jego rzecz usług na wskutek popełnienia przestępstwa. Za naruszone dobro prawne uznać należy bowiem już samą możliwość realizacji e-usług, która to możliwość podbudowywana jest konstytucyjnymi prawami do swobodnej komunikacji. Wydaje się przy tym, że nieistotna pozostaje w tym wypadku kwestia oceny, czy dany użytkownik rzeczywiście chciał skorzystać z poczty w czasie jej niedostępności, bowiem dla uznania faktycznego wystąpienia naruszenia prawa, jak wynika z redakcji art. 49 Kpk, nie jest nawet konieczna świadomość wystąpienia tego naruszenia po stronie osoby pokrzywdzonej. Dodatkowo, o pokrzywdzeniu przesądza także samo zagrożenie dobra prawnego przestępstwem.

Wysoce problematyczna staje się kwestia oceny, czy za pokrzywdzonego można

w opisywanej sytuacji uznać osobę, która w czasie ataku nie posiadała skrzynki pocztowej na atakowanym serwerze, lecz chciała ją dopiero założyć, co zostało jej uniemożliwione wskutek przestępnego zakłócenia pracy systemów. Udzielenie w tym przypadku odpowiedzi twierdzącej oznaczałoby w praktyce, że każdy atak Dos lub Ddos skierowany przeciwko powszechnie dostępnym usługom (pocztowym, informacyjnym, rozrywkowym, czy też społecznym), kierowany jest w istocie przeciwko wszystkim potencjalnym odbiorcom tej usługi - upraszczając, przeciwko wszystkim użytkownikom globalnej sieci Internet. Konstrukcję taką z pewnością trudno uznać za efektywną procesowo, czy w ogóle zasadną. Należy zatem uznać, że pokrzywdzonym atakiem typu Dos lub Ddos nie może stać się osoba nie będąca indywidualnie określonym użytkownikiem zakłóconej usługi.

Z pragmatycznego punktu widzenia, warto także nadmienić, że w praktyce, pełną wiedzę o wystąpieniu ataku posiada w istocie wyłącznie administrator zaatakowanej usługi, co w przypadku ataków mniejszej skali, które nie stają się medialnie znane, oznacza faktyczne ograniczenie dostępu pokrzywdzonych atakiem do informacji, że stali się ofiarami działań cyberprzestępczych. Wielokrotnie, brak odpowiedzi wielu usług sieciowych odczytywany jest przez użytkowników, jako zwykła awaria systemu, czy też czas wykonywania przez administratora serwera niezapowiadanych działań konserwacyjnych.

Zarysowana w powyższych akapitach problematyka wielości pokrzywdzonych stanowi jeden z wyraźnych przejawów tego, jak znane, ugruntowane od wielu lat instytucje procesowe nabierają zupełnie nowego wymiaru po wprowadzeniu ich do cyberprzestrzeni. Z żalem trzeba zauważyć, że ten nowy wymiar nie znajduje swojego odzwierciedlenia w niezbędnych zmianach prawa, które nie dotrzymuje kroku rozwojowi technicznemu.

§2. Cyberprzestępstwa związane z upublicznianiem, udostępnianiem lub rozsyłaniem w cyberprzestrzeni określonych treści lub materiałów

Druga spośród zidentyfikowanych kategorii cyberprzestępstw obejmuje czyny polegające na zamieszczaniu w sieci określonych kategorii materiałów, których szeroko rozumiane rozpowszechnianie jest zabronione, czy to z uwagi na nielegalny charakter samych materiałów, czy też wyłącznie nielegalność ich nachalnego rozsyłania (spam). O ile z technicznego punktu widzenia udostępnianie w sieci jakichkolwiek zasobów wymaga oczywiście transmisji danych, o tyle celem wyodrębnionej tu kategorii cyberprzestępstw, wyraźnie odróżniającym ją od kategorii poprzedniej (przestępstwa w ramach transmisji), jest samo uczynienie określonych zasobów dostępnymi dla innych użytkowników, czy to indywidualnie określonych, czy też należących do nieoznaczonego kręgu odbiorców.

Do katalogu tak scharakteryzowanych cyberprzestępstw związanych z upublicznianiem, udostępnianiem lub rozsyłaniem określonych treści lub materiałów, zaliczyć należy w szczególności:

1) rozsyłanie niezamówionych materiałów reklamowych, tzw. spam;
2) udostępnianie informacji uzyskanych w ramach cyberprzestępstwa, np. wykradzionych z systemu;
3) zamieszczanie w cyberprzestrzeni materiałów zabronionych prawem, w tym materiałów podżegających lub nawołujących do popełniania cyberprzestępstw, informacji mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym[105], zasługujących na szczególne potępienie tak prawne, jak i moralne, materiałów zawierających pornografię z udziałem dzieci[106], a także materiałów naruszających prawa autorskie - w szczególności nielegalnych kopii oprogramowania oraz utworów audio-wizualnych.

Ponieważ powyższe cyberprzestępstwa nie opierają się na przeprowadzaniu ataków cybernetycznych, ich analiza została ograniczona do analizy prawnej. Uzupełniająco, rozważania szczegółowe, dot. poszczególnych typów przestępstw, poprzedzone zostały ogólnym przybliżeniem sposobów dystrybucji materiałów w sieci.

1. Charakterystyka sposobów propagacji danych w cyberprzestrzeni

Jedną z podstawowych metod udostępniania wszelkiego rodzajów zasobów komputerowych za pośrednictwem sieci, jest ich zamieszczanie na stronach internetowych. W języku technicznym, dystrybucja taka odbywa się z wykorzystaniem protokołu HTTP[107] (warto zwrócić uwagę, że każdy adres internetowy strony WWW poprzedzony jest prefiksem „http://”). Zasoby dodawane są do stron bądź to, jako materiały wyświetlające się na samych stronach, to jest w oknie przeglądarki internetowej, np. zwykły tekst, zdjęcia, czy tzw. materiały strumieniowane (nagrania audio-video), bądź też jako załączone do strony pliki, których pobranie inicjowane jest poprzez naciśnięcie właściwego odsyłacza. Co do zasady, każda strona internetowa dostępna jest dla wszystkich użytkowników Internetu, jednak często określone zasoby witryn lub też nawet ich cała zawartość, dostępne są jedynie dla

[105] S. Kosmynka, Cyberdżihad. Wykorzystanie internetu przez współczesny terroryzm islamistyczny, w: A. Podraza, P. Potakowski, K. Wiak, Cyberterroryzm zagrożeniem XXI wieku, Difin, Warszawa 2013, s. 112 i nast.
[106] M. Siwicki, op. cit., 2013, s. 178 i nast.
[107] HTTP - *Hypertext Transfer Protocol.* Więcej na temat działania protokołu HTTP na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/Hypertext_Transfer_Protocol.

zarejestrowanych użytkowników strony, forum, czy też portalu. Stosowna rejestracja może przybrać postać czynności wykonywanej automatycznie (po wypełnieniu krótkiego formularza, użytkownik dostaje swój login i hasło), jednak może też wymagać indywidualnej akceptacji członkostwa ze strony administratora lub też moderatora danego systemu. Członkostwo może być oczywiście zarówno darmowe, jak i odpłatne.

Innym przykładowym sposobem dystrybucji materiałów w sieci, jest korzystanie z tzw. serwerów FTP (rolę takiego serwera może pełnić każdy komputer PC z zainstalowanym odpowiednim oprogramowaniem)[108]. Pliki umieszczone na serwerze FTP dostępne są do pobrania wyłącznie za pomocą oprogramowania nazywanego „klientem FTP". Dla zainicjowania połączenia z serwerem, pobierający musi znać adres IP serwera FTP oraz ewentualnie, jego hasło. Po zestawieniu połączenia, klient FTP uzyskuje dostęp do wybranych zasobów serwera FTP.

Z uwagi na ograniczenia techniczne charakteryzujące powyższe metody dystrybucji plików, coraz częściej sieciowa wymiana dokonywana jest z zastosowaniem darmowych usług hostingowych. W Internecie znaleźć można wiele serwisów oferujących darmową przestrzeń dyskową, która może być wykorzystywana, jako platforma wymiany zasobów (np. serwis *rapidshare*). Po utworzeniu konta w takiej usłudze oraz umieszczeniu pliku na uzyskanej przestrzeni dyskowej, jego propagacja dokonywana jest poprzez udostępnianie jedynie odsyłacza, wskazującego adres, z którego możliwe jest pobranie danego zasobu. Metoda ta często wykorzystywana jest do propagacji nielegalnych kopii utworów audio-wizualnych oraz oprogramowania. Stosowne odsyłacze znaleźć można najczęściej na dedykowanych forach internetowych.

Niezwykłą popularnością cieszą się także tzw. *torrenty*[109] oraz aplikacje oparte na modelu wymiany danych *peer-to-peer*[110] (np. *Kazaa*). Idea sieci *torrent* oparta jest na prostym pomyśle, aby poszczególni użytkownicy nie wymieniali się całymi plikami, lecz ich częściami. W ten sposób, nie tylko lepiej wykorzystuje się przepustowość dostępnych łączy, ale przede wszystkim - z punktu widzenia karnoprawnego, utrudnia przeprowadzenie kwestii

[108] FTP - *File Transfer Protocol*. Więcej na temat działania protokołu FTP na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/File_Transfer_Protocol.

[109] Więcej o protokole *BitTorrent* na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/BitTorrent.

[110] *Peer-to-peer*, zwany też P2P, to model komunikacji w sieci, w którym każdy z użytkowników posiada te same uprawnienia. W modelu tym, połączenie nie jest realizowane za pośrednictwem serwera centralnego obsługującego daną usługę, lecz bezpośrednio pomiędzy użytkownikami, w ramach tzw. samoorganizującej się sieci. Oprogramowanie P2P najczęściej działa w ten sposób, że wyszukuje określone (zadane) materiały w zasobach udostępnianych przez innych użytkowników usługi, a następnie zestawia połączenie pomiędzy tymi użytkownikami celem ich propagacji. Więcej na temat P2P na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/Peer-to-peer.

dowodowych w odniesieniu do procesu rozpowszechnienia całego materiału. Specjalna aplikacja obsługująca protokół komunikacji *BitTorrent* wyszukuje użytkowników posiadających interesujące pliki lub ich fragmenty, zgrywa je na komputer użytkownika oraz ostatecznie, zestawia w całość. Znakomita większość materiałów udostępnianych w sieciach P2P oraz sieciach *torrent* to nielegalne kopie filmów, albumów muzycznych, gier komputerowych oraz innego oprogramowania.

Ostatecznie, do rozsyłania tzw. spamu - czyli niezamawianych materiałów reklamowych, wykorzystywana jest z kolei poczta elektroniczna. Dla zautomatyzowania procesu rozsyłania maili tworzone są tzw. listy mailingowe, mogące zawierać nawet dziesiątki, czy setki tysięcy wpisów. Odpowiednio duże listy, pozwalające rozsyłać spam na masową skalę, stanowią wręcz towar sam w sobie. Spam może zawierać zarówno niegroźne treści reklamowe, jak również ukryte oprogramowanie złośliwe, mogące prowadzić nawet do przejęcia kontroli nad komputerem. Zgodnie z raportem jednego największych dostawców oprogramowania antywirusowego, szacunkowa liczba wysyłanych wiadomości typu spam przekracza globalnie 40 miliardów wiadomości dziennie (!), przy czym prawie połowa spamu to reklamy środków farmaceutycznych. Jednocześnie, średnio jeden mail na około 200, zawiera w sobie oprogramowanie złośliwe[111].

2. Rozsyłanie niezamówionych materiałów reklamowych (spam)

Wyrażenie „spam", określające niezamawiane wiadomości pocztowe, zaczerpnęło swoje korzenie od nazwy amerykańskiej mielonki, choć nie jest możliwe przesądzenie, kto pierwszy zastosował to określenie do poczty e-mail. Jako zjawisko internetowe, historia spamu jest w zasadzie tak długa, jak historia samego Internetu.

Z uwagi na ogromne rozmiary zjawiska spamu, ograniczanie rozsyłania niezamawianych wiadomości pocztowych stało się przedmiotem licznych regulacji prawnych - w tym o charakterze karnym, przyjmowanych zarówno na poziomie krajowym, jak i międzynarodowym. Przepisy nastawione na zwalczanie spamu przyjęte zostały w większości krajów całego świata, m.in. w USA[112], Kanadzie[113], Australii[114],

[111] Na podstawie Raportu Zagrożeń w Internecie firmy Symantec za rok 2011 (raport opublikowany w roku 2012). Pełen raport dostępny jest na stronie internetowej pod adresem: http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=2011_in_numbers.

[112] Tzw. ustawa *CAN-SPAM Act* z 2003 r. Pełny, oryginalny tytuł regulacji brzmi: *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*.

[113] Tzw. ustawa PIPEDA z 2000 r. Pełny, oryginalny tytuł regulacji brzmi: *Personal Information Protection and Electronic Documents Act of 2000*.

[114] Ustawa *Spam Act* z 2003 r.

Japonii[115], Izraelu[116] oraz krajach Unii Europejskiej, której podstawowym dokumentem normatywnym nastawionym na zwalczanie spamu stała się Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (tzw. dyrektywa o prywatności i łączności elektronicznej). W oparciu o przepisy wskazanej dyrektywy, stosowne regulacje anty-spamowe wprowadzone zostały także do prawa polskiego.

Zgodnie z art. 24 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[117]:

„Art. 24. 1. Kto przesyła za pomocą środków komunikacji elektronicznej niezamówione informacje handlowe, podlega karze grzywny.

2. Ściganie wykroczenia, o którym mowa w ust. 1, następuje na wniosek pokrzywdzonego.”.

Powyższą normę w sposób istotny uzupełnia przepis art. 10 ust. 1 i 2 cytowanej ustawy:

„Art. 10. 1. Zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej.

2. Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny.”.

Ostatecznie, na mocy art. 2 pkt 2 „informacją handlową” w rozumieniu przepisów ustawy jest:

„każda informacja przeznaczona bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy lub osoby wykonującej zawód, której prawo do wykonywania zawodu jest uzależnione od spełnienia wymagań określonych w odrębnych ustawach, z wyłączeniem informacji umożliwiającej porozumiewanie się za pomocą środków komunikacji elektronicznej z określoną osobą oraz informacji o towarach i usługach niesłużącej osiągnięciu efektu handlowego pożądanego przez podmiot, który zleca jej rozpowszechnianie, w szczególności bez wynagrodzenia lub innych korzyści od producentów, sprzedawców i świadczących usługi”.

Komentując normę prawną zbudowaną w oparciu o przytoczone przepisy, w pierwszej

---

[115] Ustawa z 2002 r. zatytułowana „Prawo regulujące przesyłanie określonych rodzajów wiadomości poczty elektronicznej (tytuł angielski *The Law on Regulation of Transmission of Specified Electronic Mail*).

[116] Stosowne przepisy dot. spamu wprowadzone zostały do ustawy Prawo telekomunikacyjne (m.in. nowelizacją z 2008 r.).

[117] Dz. U. Nr 144, poz. 1204, z późn. zm.

kolejności należy wskazać, że na gruncie prawa polskiego rozsyłanie niezamówionych informacji handlowych traktowane jest, jako wykroczenie (orzekanie następuje w trybie przepisów o postępowaniu w sprawach o wykroczenia), zagrożone karą grzywny. Wykroczenie to ścigane jest na wniosek pokrzywdzonego. Dla uznania zaistnienia owego czynu bezprawnego, nie jest istotne ustalenie w jaki sposób niezamawiane informacje są rozsyłane, o ile tylko wykorzystywane są do tego środki komunikacji elektronicznej. Przyjęta redakcja art. 24 ustawy o świadczeniu usług drogą elektroniczną obejmuje zatem zakresem przedmiotowym nie tylko niezamawiane wiadomości pocztowe, ale także te otrzymywane np. w ramach wszelkich grup dyskusyjnych (np. Usenet, czy BBS).

Jak wynika z ustawowej definicji informacji handlowej, za informację taką uważa się, ogólnie rzecz ujmując, wszelkie informacje nastawione na osiągnięcie efektu handlowego, a zatem reklamy, informacje o promocjach, informacje o wysokich wynikach przedsiębiorcy lub jego produktów, czy wreszcie informacje promujące określone osoby w kontekście wykonywanego przez nie zawodu. Informacja handlowa uważana jest za informację niezamówioną do czasu wyrażenia zgody na jej otrzymanie przez adresata. Zgodnie jednak z przytoczonym przepisem art. 10 ustawy, owa zgoda może zostać wyrażona nawet w sposób dorozumiany, w szczególności poprzez udostępnienie adresu poczty elektronicznej. Rozwiązanie to należy oceniać, jako niezapewniające należytego poziomu ochrony przed nieuprawnionym wyrażeniem zgody na otrzymywanie wiadomości w imieniu innej osoby (wystarczy wpisać cudzy adres e-mail w odpowiednim polu na stronie WWW, nie składając przy tym żadnych oświadczeń).

Porównując redakcję przepisów art. 10 i 24 ustawy o świadczeniu usług drogą elektroniczną, nie sposób nie zauważyć występującej pomiędzy nimi niekompatybilności. O ile art. 10 wprowadza zakaz „przesyłania niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy", o tyle na gruncie art. 24 uregulowana jest ogólna o penalizacja „przesyłania za pomocą środków komunikacji elektronicznej niezamówionej informacji handlowej" - bez wskazania, że i w tym przypadku chodzi o oznaczonego odbiorcę. Traktując zatem normę art. 24 ustawy, jako samodzielny przepis karny (wprowadzony do rozdziału zatytułowanego „Przepisy karne"), można dojść do absurdalnego wniosku, że na gruncie polskiego prawa karane jest przesyłanie w cyberprzestrzeni wszelkich niezamawianych reklam, w tym reklam, które pojawiają się na stronach internetowych bez naszej zgody. Wskazana niespójność stanowi wyraz niskiej jakości legislacyjnej ustawy.

Za pokrzywdzonego, o którym mowa w art. 24 ustawy o świadczeniu usług drogą elektroniczną należy uznawać każdą osobę, która otrzymała niezamówioną informację

handlową, w tym także osobę, która otrzymała taką informację na wskutek nieuprawnionego wyrażenia zgody w jej imieniu. Z uwagi na faktyczne rozmiary zjawiska rozsyłania poczty kwalifikowanej jako spam, rozwiązanie to może oznaczać w praktyce nawet setki tysięcy osób pokrzywdzonych wysłaniem jednej wiadomości e-mail, uprawniając każdą z nich do złożenia wniosku o ściganie. Rozwiązanie to powoduje oczywiście szereg konsekwencji procesowych w przypadku składania przez pokrzywdzonych dużej liczby wniosków w różnym czasie oraz w różnych miejscach. W przypadku spamu zawierającego oprogramowanie złośliwe, kierowanego do urzędów administracji publicznej lub też przekraczającego pewną skalę, zasadne wydaje się wprowadzenie trybu ścigania z urzędu.

3. Udostępnianie informacji uzyskanych w ramach cyberprzestępstwa

Na mocy art. 267 § 4 Kk, do krajowego porządku prawnego wprowadzona została norma ogólna penalizującą ujawnianie informacji, które zdobyte zostały w toku popełnienia cyberprzestępstwa - w szczególności szeroko rozumianego *hackingu* oraz podsłuchu treści transmisji, stypizowanych w art. 267 § 1 - 3 Kk. Poniżej treść całego art. 267 Kk:

> „Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
>
> § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
>
> § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
>
> § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.
>
> § 5. Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego.”.

Wychodząc od krótkiej redakcji art. 267 § 4 Kk, zbudować można następującą normę prawną nastawioną na penalizację nieuprawnionego ujawniania informacji zdobytych w toku popełnienia cyberprzestępstwa[118]:

---

[118] A. Lach, op. cit., system LEX - komentarz do art. 267 k.k., W. Wróbel, op. cit., system LEX - komentarz do art. 267 k.k.

- komentowana norma dotyczy ujawniania informacji, które uzyskane zostały w sposób nieuprawniony poprzez: otwarcie zamkniętego pisma, podłączenie się do sieci telekomunikacyjnej, przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia (za § 1), uzyskanie dostępu do całości lub części systemu informatycznego (za § 2) lub też zakładanie lub posługiwanie się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem (za § 3),
- dla zaistnienia przestępstwa, stypizowanego w art. 267 § 4 Kk nie ma znaczenia ani rodzaj, ani charakter, ani też sposób ujawnienia wykradzionej informacji. W szczególności nie istotne jest to, czy przedmiotowa informacja jest ważna lub cenna dla jej właściciela lub też osoby wchodzącej w jej posiadanie w sposób nieuprawniony. Wystarczający jest tu sam fakt, że ujawniana dalej informacja uzyskana została w ramach wcześniejszego przeprowadzenia określonych działań przestępnych. Jednocześnie, ujawniana informacja może być wyrażona w dowolnej formie: czy to pisemnej (dokumenty tekstowe, arkusze kalkulacyjne, hasła, kody źródłowe), audio-wizualnej (zdjęcia, nagrania filmowe), czy też wykonywalnej przez komputer (zawartej w oprogramowaniu lub też stanowiącej oprogramowanie). Bez znaczenia dla kwalifikacji przestępstwa stypizowanego art. 267 § 4 Kk pozostaje także sposób w jaki informacja komunikowana jest innej osobie - czy to za pośrednictwem systemu teleinformatycznego (np. poprzez przesłanie wykradzionych materiałów pocztą elektroniczną), czy na informatycznym nośniku danych (np. poprzez wręczenie nielegalnej kopii bazy danych, która zgrana została na płytę CD), czy też w ogóle poza systemami - pisemnie lub nawet ustnie,
- zastosowane w redakcji § 4 znamię „ujawnia innej osobie" należy rozumieć, jako konstytuujące przestępstwo materialne, którego faktyczne zaistnienie wymaga wystąpienia określonego skutku. W analizowanym przypadku, skutkiem tym jest zapoznanie się osoby nieuprawnionej - innej niż sprawca, z treścią opisywanej wyżej informacji[119],
- co było wskazywane już wcześniej, wprowadzenie do redakcji art. 267 Kk pojęcia „informacji" powoduje, że ujawnienie innej osobie danych komputerowych nie stanowiących informacji - w szczególności danych zaszyfrowanych, których odczytanie nie jest możliwe w momencie ich przekazywania, nie wypełnia znamion

[119] J. Piórkowska-Flieger, op. cit., s. 591.

czynu opisanego w § 4 komentowanego przepisu. Rozwiązanie to należy oceniać jako wysoce wadliwe oraz nie znajdujące swojego odzwierciedlenia w przepisach aktów ponadnarodowych (m.in. w wielokrotnie przywoływanej Konwencji o cyberprzestępczości, w której stosowane jest pojęcie „danych komputerowych") - *vide* uwagi zawarte w części 1 niniejszego rozdziału.

Powyższe przestępstwo może ponadto pozostawać w zbiegu z czynem opisanym w art. 269b § 1 Kk, w przypadku, gdy dotyczy ono informacji w postaci uprzednio wykradzionych haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do dowolnego systemu. Należy zauważyć, że jednym z działań zawodowych hackerów jest włamywanie się do systemów na zlecenie, celem uzyskania haseł dostępowych umożliwiających podgląd określonych kategorii danych (np. inwigilację cudzego konta pocztowego, czy też wgląd w informacje wymieniane z zastosowaniem komunikatorów internetowych) lub też wprowadzenie w obranym za cel systemie autoryzowanych od strony technicznej, choć w dalszym ciągu formalnie nieuprawnionych zmian. Regulacja art. 269b Kk prezentowana jest szerzej w części 2. rozdziału.

4. Zamieszczanie w cyberprzestrzeni materiałów zabronionych prawem

W ramach przedmiotowej kategorii przybliżane są obowiązujące w Polsce regulacje karne nastawione na zwalczanie wykorzystywania cyberprzestrzeni, jako narzędzia do propagacji następujących kategorii materiałów:

a) materiałów podżegających lub nawołujących do popełniania cyberprzestępstw,
b) materiałów mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym (np. dotyczących sporządzania broni i materiałów wybuchowych),
c) zasługujących na szczególne potępienie, materiałów zawierających pornografię udziałem dzieci, oraz
d) nielegalnych kopii oprogramowania komputerowego, pozostającego pod ochroną prawnoautorską.

Zastosowane w śródtytułach wyrażenie „zamieszczanie", rozumiane jest w sposób techniczny, jako każdy przejaw wprowadzenia określonego zasobu do cyberprzestrzeni.

Zamieszczanie w cyberprzestrzeni materiałów podżegających lub nawołujących do popełniania cyberprzestępstw

Jednym z najniebezpieczniejszych współczesnych trendów tzw. *haktywizmu*[120] (mianem tym określa się nielegalną działalność hackerską nastawioną na osiągnięcie określonych celów *(pseudo-?)*społecznych lub nawet *(pseudo-?)*politycznych) stało się dziś organizowanie przez rozległe grupy hackerskie szeroko zakrojonych ataków cybernetycznych przeprowadzanych przy aktywnym oraz świadomym współudziale osób trzecich. Przy działaniach tego typu hackerzy tworzą oraz udostępniają w sieci narzędzia informatyczne mające umożliwić przeprowadzenie ataku oraz wzywają Internautów do wzięcia udziału w akcji poprzez przyłączenie się (a dokładniej rzecz ujmując - przyłączenie swojego komputera) do sieci komputerów, które zostaną wykorzystane do przeprowadzenia określonego ataku (przygotowywana jest swojego rodzaju sieć Botnet). Akcje takie odbywają się najczęściej pod hasłami walki o wolność, prawa obywateli do prywatności oraz ogólnie rozumianej „walki z systemem". Niektóre z nich przybierają wręcz postać ataków politycznych, nakierowanych przeciwko określonym działaniom rządu (jak było w przypadku ataków przeprowadzonych na okoliczność podpisania międzynarodowej umowy handlowej dotyczącej zwalczania obrotu towarami podrabianymi[121] - w skrócie tzw. ACTA).

Art. 11 Konwencji Rady Europy o cyberprzestępczości, który to przepis zatytułowany został „Usiłowanie oraz pomocnictwo i podżeganie"[122], stanowi w swoim ust. 1, że:

> „Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego, umyślnego pomocnictwa w popełnieniu lub podżegania do popełnienia, przestępstw określonych w art. 2 - 10 niniejszej Konwencji, z zamiarem, że takie przestępstwo zostanie popełnione."[123].

Przestępstwa określone w art. 2 - 10 Konwencji to: uzyskanie dostępu do systemu,

---

[120] Samo wyrażenie powstało z połączenie słów *hacking* oraz *activism*. Więcej na temat jego znaczenia na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Hacktivism. O zjawisku pisano także szerzej w rozdziale I pracy.

[121] Tytuł oryginalny umowy: „*Anti-Counterfeiting Trade Agreement*".

[122] W oryginale: „*Attempt and aiding or abetting*". Używany w języku angielskim łącznie zwrot „*aid and abet*" po przeniesienie na grunt polskiego języka prawnego tłumaczyć należy, jako „pomocnictwo oraz podżeganie". Tłumaczenie własne. Tak też np.: P. Waglowski, w swoim tłumaczeniu komentowanego zapisu na stronie internetowej dostępnej pod adresem: http://prawo.vagla.pl/skrypts/cybercrime_konwencja.htm. W oficjalnym tłumaczeniu Konwencji przedmiotowy zwrot zapisano analogicznie, w brzmieniu „usiłowanie i pomocnictwo lub podżeganie".

[123] Art. 11 ust. 1 Konwencji o cyberprzestępczości. W oryginale: „*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.*". Tłumaczenie własne.

przechwytywanie danych, ingerencja w dane, zakłócenie pracy systemu, bezprawne wykorzystanie urządzenia, fałszerstwo komputerowe, oszustwo komputerowe, przestępstwa związane z pornografią dziecięcą oraz naruszenia praw autorskich. Katalog ten obejmuje wszystkie rodzaje cyberprzestępstw określonych w konwencji budapesztańskiej (choć można także rozważać, czy samo podżeganie do podżegania, czyli tzw. podżeganie łańcuszkowe[124] - problem wcale nie tylko teoretyczny w świetle pseudo-społecznych akcji grup hackerskich, jak np. grupy *Anonymous* - również nie powinno być objęte szczególną penalizacją w kontekście cyberbezpieczeństwa).

Zgodnie z analogicznym zapisem Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[125], zawartym w art. 5 ust. 1 decyzji, na gruncie prawodawstwa unijnego przyjęto pierwotnie, że:

> „Art. 5. 1. Każde Państwo Członkowskie zapewnia, że kierowanie, pomaganie i podżeganie do przestępstw, o których mowa w art. 2, 3 i 4, jest karane jak przestępstwo.”.

W osiem lat później, na gruncie przepisów Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne[126] - zastępującej postanowienia Decyzji Ramowej, prawodawca Unijny zapisał w art. 8 przywołanego dokumentu, iż

> „1. Państwa członkowskie zapewniają, aby podżeganie do przestępstw, o których mowa w art. 3–7, oraz pomocnictwo w tych przestępstwach było karalne jako przestępstwo.
>
> 2. Państwa członkowskie zapewniają, aby usiłowanie popełnienia przestępstw, o których mowa w art. 4 i 5, było karalne jako przestępstwo.”

O ile w każdym z przytaczanych przypadków, regulacje dotyczące karalności podżegania oraz pomocnictwa poszczególnych kategorii czynów objęły całokształt przestępstw opisywanych w komentowanych dokumentach, o tyle z regulacji Dyrektywy wyłączone zostało normowanie *expressis verbis* karalności kierowania. Przepis Dyrektywy wprowadził natomiast dodatkową normę, nakazującą zapewnienie karalności także usiłowania czynów polegających na zakłóceniu pracy systemu oraz ingerencji w dane.

Mając na uwadze powyższe regulacje, ustawodawca Polski nie zdecydował się na

---

[124] Na kontrowersyjność uznania karalności podżegania łańcuszkowego na gruncie polskiego Kodeksu karnego uwagę zwraca T. Bojarski w: T. Bojarski, A. Michalska-Warias, J. Piórkowska-Flieger, M. Szwarczyk, Kodeks karny. Komentarz, LexisNexis, wydanie 3, Warszawa 2009, s. 69 i nast.

[125] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW.

[126] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

wprowadzenie przepisów szczególnych, które miałyby w sposób odrębny penalizować podżeganie lub nawoływanie do popełniania cyberprzestępstw, pozostawiając kwestie te przepisom o charakterze ogólnym. W związku z tym, karalność podżegania do popełnienia cyberprzestępstw na gruncie polskiego Kodeksu karnego, odbywa się w oparciu o postanowienia przepisów art. 18 - 24 Kk, ustalających ogólne zasady odpowiedzialności karnej podżegacza oraz pomocnika. Kwestia karalności podżegania do popełnienia poszczególnych cyberprzestępstw w polskim prawie oceniana musi być zatem przez pryzmat analizowanych w niniejszym rozdziale przepisów karnych przewidujących karalność poszczególnych czynów oraz z uwzględnieniem ogólnych zasad prawa karnego - z uwagi na zakres tematyczny pracy, przybliżenie ogólnych zasad prawa karnego uznano za wykraczające poza przyjęte ramy opracowania. Warto w tym miejscu jedynie nadmienić, że zgodnie z brzmieniem art. 19 § 1 Kk kara za podżeganie do popełnienia przestępstwa wymierzana jest w zakresie przewidzianym dla sprawstwa.

W kontekście poruszonego wyżej hacktywizmu, szczególnie istotnym przepisem obowiązującym na gruncie polskiej ustawy pozostaje art. 255 Kk, penalizujący nawoływanie oraz publiczne pochwalanie popełniania przestępstw. O ile udowodnienie podżegania wymaga wykazania po stronie podżegacza działalności polegającej na „nakłanianiu" do popełnienia danego przestępstwa, o tyle nawoływanie, a w szczególności pochwalanie, uznać należy za formy znacznie łagodniejsze, a co za tym idzie - zdecydowanie szersze przedmiotowo. Zgodnie z art. 255 Kk:

> „Art. 255. § 1. Kto publicznie nawołuje do popełnienia występku lub przestępstwa skarbowego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
>
> § 2. Kto publicznie nawołuje do popełnienia zbrodni, podlega karze pozbawienia wolności do lat 3.
>
> § 3. Kto publicznie pochwala popełnienie przestępstwa, podlega grzywnie do 180 stawek dziennych, karze ograniczenia wolności albo pozbawienia wolności do roku.".

Za publiczne nawoływanie uznać należy każdy przejaw wzywania bliżej nieokreślonego kręgu adresatów do podjęcia określonych działań, w tym wypadku przestępnych. Przesłankę „publicznego" charakteru owego nawoływania w szczególności spełnia zamieszczenie określonego wezwania w ogólnodostępnych zasobach cyberprzestrzeni (np. na otwartej stronie WWW, czy też publicznym forum internetowym). Forma samego wezwania pozostaje tu bez znaczenia - może to być zarówno informacja pisemna, nagranie audio-wizualne, jak też samo wskazanie celu ataku (np. adresu strony WWW) w przypadku, gdy okoliczności sprawy

jednoznacznie wskazują na treść przekazu - wezwanie do popełnienia przestępstwa. Co istotne, w odróżnieniu od redakcji art. 18 § 2 Kk, gdzie w kontekście odpowiedzialności karnej podżegacza mowa jest o nakłanianiu do „popełnienia czynu zabronionego", art. 255 Kk posługuje się zastępczo pojęciem „popełnienia przestępstwa", co wyłącza (w ocenie Autora niniejszej dysertacji - błędnie) z jego zakresu przypadki nawoływania do popełnienia czynu, który z przyczyn formalnych nie może stać się przestępstwem, np. z powodu niepoczytalności sprawcy.

Dla uznania karalności nawoływania do popełnienia przestępstwa nie jest wreszcie także istotne to, czy nawołujący wzywał do popełnienia ściśle opisanego czynu (np. przeprowadzenia samodzielnego ataku Dos, czy wzięcia udziału w rozproszonym ataku Ddos, o określonej godzinie, wobec określonej usługi sieciowej), czy też ogólnie wzywał do popełnienia przestępstwa lub przestępstw, np. dla wyrażenia swojego sprzeciwu wobec określonych wartości bądź działań[127].

Art. 255 § 3 Kk sankcjonuje z kolei „pochwalanie popełnienia przestępstwa", co odnosić należy tak do przestępstw już popełnionych, jak również tych, które dopiero mają, bądź jedynie mogą zostać popełnione. Należy podzielić pogląd głoszący, że wyrażenie pochwały popełnienia przestępstwa nie może być uznawane za tożsame z nawoływaniem do samego popełnienia przestępstwa[128]. Analogicznie, jak w przypadku nawoływania do popełnienia przestępstwa, także i pochwała jego popełnienia musi być wyrażona publicznie. Pełne zastosowanie znajdują tu więc powyższe uwagi dot. publicznego charakteru zasobów cyberprzestrzeni oraz możliwych form przekazu informacji.

Co istotne, przestępstwa stypizowane w art. 255 Kk pozostają w dość szczególnym zbiegu z regulacją art. 52a Kodeksu wykroczeń, który to przepis stanowi, że:

„Art. 52a. Kto:

1) publicznie nawołuje do popełnienia przestępstwa lub przestępstwa skarbowego,

2) publicznie nawołuje do przeciwdziałania przemocą aktowi stanowiącemu źródło powszechnie obowiązującego prawa Rzeczypospolitej Polskiej,

3) publicznie pochwala popełnienie przestępstwa,

jeżeli zasięg czynu albo jego skutki nie były znaczne – podlega karze aresztu, ograniczenia wolności albo grzywny.".

Należy zatem podzielić pogląd, że dla zaistnienia przestępstwa opisanego w art. 255 Kk konieczne jest aby oceniany czyn - w odróżnieniu od regulacji przyjętej na gruncie Kodeksu

---

[127] J. Piórkowska-Flieger, op. cit., s. 556.
[128] *Ibidem*, s. 556.

wykroczeń, posiadał „znaczny zasięg” lub też miał „znaczne skutki”. W innym przypadku, kwalifikowany powinien bowiem stanowić wykroczenie, nie zaś przestępstwo. Jak podkreśla się w doktrynie, oceny „znaczności” zasięgu oraz skutków trzeba dokonywać z uwzględnieniem kryterium rozległości obszaru oraz ilości osób, pozostających pod wpływem publicznych nawoływań lub też pochwał popełnienia przestępstwa[129]. W odniesieniu do cyberprzestrzeni, kryterium obszaru (rozumiane geograficznie, a więc nie znajdujące praktycznego zastosowania w cyberprzestrzeni) należy zastąpić kryterium ilości witryn internetowych, for, portali, czy też kanałów czat, czy IRC, które użyte zostały do publikowania określonych informacji.

Wszystkie czyny określone w art. 255 Kk stanowią przestępstwa formalne, a zatem dla ich ukonstytuowania nie jest istotne stwierdzenie wystąpienia określonego skutku, w postaci np. popełnienia przestępstwa, czy też internalizacji określonych bezprawnych zachowań.

Rozpowszechnianie w cyberprzestrzeni materiałów mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym

Istotnym *novum* 2011 r. stało się wprowadzenie do polskiej ustawy karnej przepisu penalizującego rozpowszechnianie treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym. Dodany na mocy noweli z dnia 29 lipca 2011 r.[130] przepis art. 255a Kodeksu karnego otrzymał następujące brzmienie:

> „Art. 255a. Kto rozpowszechnia lub publicznie prezentuje treści mogące ułatwić popełnienie przestępstwa o charakterze terrorystycznym w zamiarze, aby przestępstwo takie zostało popełnione, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.”.

Pomimo iż przytoczony przepis nie odwołuje się do rozpowszechniania określonych w nim materiałów za pośrednictwem cyberprzestrzeni, jego praktyczny zakres przedmiotowy w ogromnej mierze odnosi się do propagacji treści właśnie z zastosowaniem tego medium. Z uwagi na globalny zasięg Internetu oraz jego omalże powszechną dziś dostępność, cyberprzestrzeń coraz częściej wykorzystywana jest także przez grupy terrorystyczne, mogące wykorzystywać sieć do szybkiego, taniego oraz relatywnie bezpiecznego (nie wymagającego bezpośredniego kontaktu) przekazywania informacji, np. nawołujących do popełnienia przestępstwa, czy też wskazujących metodę jego przeprowadzenia. Obok najbardziej medialnych informacji dot. wskazówek, jak wyprodukować materiały wybuchowe, art. 255a

[129] *Ibidem*, s. 557.

[130] Ustawa z dnia 29 lipca 2011 r. o zmianie ustawy — Kodeks karny, ustawy — Kodeks postępowania karnego oraz ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz. U. Nr 191, poz. 1135).

Kk może zostać wykorzystany także do penalizacji czynów polegających na wskazywaniu, w jaki sposób posłużyć się określonym programem komputerowym w celu przeprowadzenia ataku cyberterrorystycznego (ataku terrorystycznego w cyberprzestrzeni) lub też samym udostępnianiu specjalnie spreparowanych programów w celu zwiększenia skali ataku terrorystycznego.

Zgodnie z treścią przypisu Nr 1 zawartego w samej noweli Kodeksu karnego wprowadzającej art. 255a, dodanie analizowanego przepisu stanowi uzupełnienie implementacji do ustawy krajowej postanowień decyzji ramowej Rady 2008/919/WSiSW z dnia 28 listopada 2008 r. zmieniającej decyzję ramową 2002/475/WSiSW w sprawie zwalczania terroryzmu[131]. Na gruncie wskazanej decyzji zmieniającej, państwa członkowskie UE zostały zobowiązane do ustanowienia w swoich krajowych porządkach prawnych karalności między innymi następujących czynów, jako „przestępstw związanych z działalnością terrorystyczną":

1) publiczne nawoływanie do popełniania przestępstw terrorystycznych;
2) rekrutacja na potrzeby terroryzmu; oraz,
3) szkolenie terrorystyczne.

Jednocześnie, zgodnie z nowym brzmieniem znowelizowanego art. 4 decyzji ramowej w sprawie zwalczania terroryzmu, każde z państw członkowskich zostało zobligowane, „aby zapewnić karalność czynów polegających na pomocnictwie w popełnieniu jednego z przestępstw, o których mowa w art. 1 ust. 1, art. 2 lub 3.". Wskazane na końcu przepisu jednostki redakcyjne (art. 1 ust. 1, art. 2 oraz 3 decyzji) obejmują wszelkie typy przestępstw, jakie zostały stypizowane w decyzji Rady Unii Europejskiej. Do przestępstw tych zaliczają się przestępstwa terrorystyczne, przestępstwa dotyczące grupy terrorystycznej oraz przestępstwa związane z działalnością terrorystyczną (wspomagające działania terrorystyczne).

Należy zaznaczyć, że wielokrotnie przywoływana w pracy Konwencja o cyberprzestępczości w żadnym ze swoich postanowień nie porusza bezpośrednio karalności przestępstw związanych z działalnością terrorystyczną.

Komentując polską regulację art. 255a Kk w kontekście zwalczania cyberprzestępczości, w pierwszej kolejności wypada stwierdzić, że jej ograniczony względem decyzji Rady UE zakres przedmiotowy, wynika z faktu iż dodany przepis stanowi jedynie jeden z elementów krajowego systemu karnego, nastawionych na zwalczanie zagrożeń

[131] Dz. Urz. UE L 330 z 09.12.2008, str. 21.

terrorystycznych. Analizowany przepis miał na celu uzupełnienie obowiązujących już regulacji o nowe rodzaje przestępstw polegających na rozpowszechnianiu materiałów „mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym". Pod pojęciem tym należy rozumieć w szczególności udzielanie instruktażu w zakresie stosowania określonych metod lub technik do popełnienia przestępstwa terrorystycznego[132], jak również udostępnianie specjalnie przygotowanych narzędzi informatycznych ułatwiających przeprowadzenie ataku - funkcjonalnie powiązane z rekrutacją (osoby pobierające narzędzie oraz następnie wykorzystujące je zgodnie z udzieloną instrukcją, stają współsprawcami ataku). Podkreślić trzeba w tym miejscu, że wiele spośród powszechnie dostępnych oraz codziennie wykorzystywanych programów komputerowych może zostać wykorzystanych do przeprowadzenia ataku, pomimo, że ich oryginalna, przewidywana przez autorów funkcjonalność, nie zakładała takiego zastosowania. Rozpowszechnianie informacji, określających w jaki sposób posłużyć się takim programem dla osiągnięcia efektu przestępnego, uznać należy właśnie za ułatwianie popełnienia przestępstwa (choćby informacja, jak wykorzystać określone funkcje systemu operacyjnego celem przeprowadzenia ataku terrorystycznego). Jednocześnie, czyn polegający na rozpowszechnianiu narzędzi informatycznych specjalnie przygotowanych do popełnienia przestępstwa o charakterze terrorystycznym pozostaje także w zbiegu z czynem stypizowanym w art. 268a Kk, prezentowanym szerzej w dalszym punkcie 5 niniejszej części rozdziału, polegającym na propagacji narzędzi służących do przeprowadzania wszelkiego rodzaju ataków w cyberprzestrzeni.

Zgodnie z regulacją kodeksową, znamionami przestępstwa opisanego w art. 255a są „rozpowszechnianie" oraz „publiczna prezentacja" treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym. Obydwa wymienione pojęcia odnoszą się przede wszystkim do udostępniania określonych informacji nieoznaczonemu kręgowi adresatów, choć funkcjonalnie z zakresu semantycznego wyrazu „rozpowszechnianie" - w ocenie Autora niniejszej rozprawy - nie należy wyłączać dystrybucji materiałów do osób oznaczonych (np. w sytuacji, w której materiały publikowane są na zamkniętym forum, do którego dostęp uzyskuje się na podstawie znajomości sekretnego hasła). W doktrynie często wyrażany jest jednak pogląd przeciwny (rozpowszechnianie wyłącznie w kontekście nieograniczonego kręgu adresatów)[133]. Kolejną kwestią dyskusyjną, również wciąż oczekującą na wyjaśnienie

[132] W ten sposób na gruncie przywoływanej decyzji ramowej w sprawie zwalczania terroryzmu definiowane jest pojęcie „szkolenia terrorystycznego".
[133] Na kwestię tę uwagę zwraca A. Adamski w: Cyberprzestępczość..., op. cit., s. 67.

przez ustawodawcę, pozostaje także pytanie, czy słowo „rozpowszechnianie" winno być rozumiane, jako nieprzesądzające uzyskania efektu w postaci przekazania określonej informacji osobie trzecie? Innymi słowy - czy dla stwierdzenia zaistnienia przesłanki „rozpowszechniania" konieczne, jest aby udostępniona informacja została rzeczywiście przez kogokolwiek odczytana, czy też wystarczający jest sam fakt jej zamieszczenia w miejscu dostępnym dla innych osób (użytkowników systemu)? Warto zauważyć, że w odniesieniu do specyfiki cyberprzestrzeni - na poziomie technicznym, rozpowszechnienie materiału dokonywane jest w momencie jego wprowadzenia do pamięci systemu teleinformatycznego nie zaś w momencie jego odebrania, bądź też odczytania przez osobę trzecią. Sytuację tę potęguje fakt, że wiele serwerów obsługujących strony internetowe wykonuje tzw. kopie zapasowe danych na wypadek wystąpienia awarii systemu. Zatem nawet treści, które zostaną umieszczone w sieci (na stronie lub forum) tylko na chwilę, po czym za moment usunięte, mogą być już powielone oraz odczytane w późniejszym terminie, w przypadku przywrócenia danych z owej kopii zapasowej. W ocenie autora pracy, powyższe argumenty przemawiają za rozumieniem słowa „rozpowszechnianie" - w obszarze cyberprzestrzeni, w sposób *samodzielny*, tzn. w oderwaniu od koniecznego do wystąpienia skutku (rozpowszechnianie, jako czynność faktyczna, formalna). Pogląd ten uznać trzeba jednak za *novum* odbiegające od utartych standardów, niestety nie zawsze przystających do zmieniającej się rzeczywistości[134].

Ostatecznie, aby określony czyn móc zakwalifikować, jako przestępstwo, o którym mowa w art. 255a Kk, czyn ten musi zostać popełniony w szczególnym zamiarze: to jest, aby popełnione zostało przestępstwo o charakterze terrorystycznym. Innymi słowy, zwykła publikacja informacji o możliwości *nadużycia* określonych funkcjonalności oprogramowania do wywołania dysfunkcji wybranego systemu teleinformatycznego nie może być kwalifikowana, jako przestępstwo stypizowane w art. 255a Kk, o ile brak jest możliwości wykazania związku pomiędzy ową publikacją, a jej celem, jakim ma być chęć doprowadzenia do popełnienia przestępstwa o charakterze terrorystycznym. Jednocześnie, dla zaistnienia przestępstwa z art. 255a Kk nie jest istotne, czy owo przestępstwo o charakterze terrorystycznym (przestępstwo docelowe) zostało faktycznie popełnione.

[134] Np. wyrok Sądu Najwyższego z dnia 16 lutego 1987 r., WR 28/87, OSNKW 19987, nr 9-10, poz. 85, w którym stwierdzono, że rozpowszechnianiem nie jest udostępnianie treści ściśle określonemu kręgowi ich odbiorców. Przywołuję za: J. Piórkowska-Flieger, op. cit., s. 420.

Rozpowszechnianie w cyberprzestrzeni materiałów zawierających pornografię z udziałem dzieci

Bez wątpienia jedną z najciemniejszych stron cyberprzestrzeni stały się portale oraz fora internetowe oferujące swoim użytkownikom dostęp do tzw. pornografii z udziałem dzieci. Z uwagi na powszechną pośród społeczności internetowej dezaprobatę wobec materiałów pornograficznych z udziałem nieletnich, owe portale oraz fora stanowią element tzw. podziemia internetowego, ukrywającego się nie tylko przed organami ścigania, ale także wszelkimi osobami postronnymi. Warto zaznaczyć, że witryny internetowe propagujące pornografię z udziałem dzieci coraz częściej stają się celem cyberataków organizowanych przez profesjonalne grupy hackerskie[135] (działalność *hacktywistyczna*). Z uwagi na charakter niniejszego opracowania - skupiającego się na kwestiach szczególnych z punktu widzenia zwalczania cyberprzestępczości, analizę samego pojęcia „pornografia dziecięca" pozostawiam poza zakresem prowadzonych rozważań.

Uznając konieczność zapewnienia organom ścigania skutecznych narzędzi zwalczania pornografii dziecięcej, dystrybucja materiałów pornograficznych z udziałem nieletnich w obszarze cyberprzestrzeni stała się przedmiotem szczególnych, specjalistycznych regulacji prawnokarnych, wprowadzanych na poziomie zarówno krajowym, jak i międzynarodowym[136]. Jednym z najistotniejszych przejawów legislacji międzynarodowej w tym zakresie są przepisy Konwencji Rady Europy o cyberprzestępczości.

Zgodnie z budową Konwencji, kwestia karalności przestępstw powiązanych z pornografią dziecięcą uregulowana została w art. 9, wchodzącym w skład tytułu III o nazwie „przestępstwa związane z przetwarzanymi treściami"[137]. Wskazany przepis otrzymał następujące brzmienie:

„Art. 9 1. Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego, popełnionego umyślnie, bezprawnego czynu polegającego na:

a wytwarzaniu pornografii dziecięcej w celu jej dystrybucji za pośrednictwem systemu komputerowego;

b oferowaniu lub czynieniu dostępnym pornografii dziecięcej za pośrednictwem

[135] Przykładowe doniesienia o cyberatakach na witryny internetowe zawierające materiały pornograficzne z udziałem nieletnich dostępne są na stronach: http://www.bbc.co.uk/news/technology-15428203, http://www.dailymail.co.uk/sciencetech/article-2053774/Hacker-group-Anonymous-performs-vigilante-attack-online-child-porn-hub.html, czy też nieco starsze (datowane jeszcze na 1998 r.) http://news.cnet.com/2100-1023-207725.html.

[136] M. Siwicki, op. cit., s. 178 i nast.

[137] W oryginale: „*Content-related offences*". Tłumaczenie własne.

systemu komputerowego;

c dystrybuowaniu lub przesyłaniu pornografii dziecięcej za pośrednictwem systemu komputerowego;

d pozyskiwaniu pornografii dziecięcej za pośrednictwem systemu komputerowego dla siebie lub innej osoby;

e posiadaniu pornografii dziecięcej w systemie komputerowym lub na nośniku przechowywania danych komputerowych.

2. W rozumieniu powyższego paragrafu 1, wyrażenie „pornografia dziecięca" obejmuje materiały pornograficzne ukazujące wizualnie:

a nieletniego biorącego udział w wyraźnych czynności seksualnych;

b osobę ukazywaną jako nieletnia biorącą udział w wyraźnych czynnościach seksualnych;

c realistyczne obrazy prezentujące nieletniego biorącego udział w wyraźnych czynnościach seksualnych.

3. W rozumieniu powyższego paragrafu 2, wyrażenie „nieletni" oznacza osobę poniżej 18 roku życia. Strona może ustanowić niższą granicę wieku, jednak nie poniżej 16 lat.

4. Każda Strona może zastrzec prawo do niestosowania, w całości lub części, lit. d i e paragrafu 1 oraz lit. d i c paragrafu 2."[138].

Z uwagi na obszar regulacyjny Konwencji, wszystkie stypizowane w niej *przestępstwa powiązane z pornografią dziecięcą* odniesione zostały do przetwarzania materiałów zawierających taką pornografię w systemach komputerowych. Zgodnie z redakcją przytoczonego przepisu, na mocy Konwencji usankcjonowane zostało wytwarzanie oraz oferowanie pornografii dziecięcej, jej szeroko rozumiane udostępnianie, dystrybuowanie, przesyłanie, pozyskiwanie oraz samo posiadanie. W kontekście propagowania pornografii

[138] W oryginale: *„1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct. 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.".* Tłumaczenie własne. W oficjalnym przekładzie Konwencji czyny przestępne opisane w ust. 1 zostały stypizowane w kolejnych punktach, z zastosowaniem następujących określeń dla działań sprawczych wobec pornografii dziecięcej: a. produkowanie, b. oferowanie lub udostępnianie, c. rozpowszechnianie lub transmitowanie, d. pozyskiwanie, e. posiadanie.

dziecięcej w cyberprzestrzeni, wyliczony katalog czynności należy uznać za pełny, *de facto* obejmujący wszelkie formy technicznego przetwarzania danych w systemach teleinformatycznych (na gruncie Konwencji - systemach komputerowych). W szczególności zatem przyjęta została karalność:

1) samego posiadania dowolnego zapisu pornografii dziecięcej w systemie - tak w pamięci ulotnej komputera (RAM), jak i na dowolnym nośniku danych (dysku twardym, płycie CD, pamięci typu *flash*, itd.) - w tym dysku sieciowym, który może być zlokalizowany w dowolnym punkcie cyberprzestrzeni (inaczej mówiąc – w dowolnym punkcie na globie);
2) pobierania zasobów zawierających pornografię z udziałem dzieci (§ 1 lit. d stanowiący o *pozyskiwaniu*, rozumianym w szczególności, jako zwykłe pobieranie danych z sieci[139]);
3) dystrybuowania - rozumianego, jako aktywne rozpowszechnianie[140], zakładające czynny udział sprawcy propagującego pornografię z udziałem dzieci (np. organizacja portalu internetowego oferującego treści pornograficzne z udziałem małoletniego);
4) oferowania - rozumianego szeroko, jako wszelkie przejawy udostępniania pornografii z udziałem dzieci, także np. w postaci odnośnika zapisanego na stronie internetowej, odsyłającego do adresu docelowego zawierającego materiały pornograficzne[141]; oraz,
5) przesyłania - rozumianego ogólnie, jako wszelkie formy wysyłania danych pomiędzy systemami[142], w tym transmisję danych pobieranych ze stron internetowych lub wysyłanych do umieszczenia na takich stronach, jak również transmisję poczty elektronicznej, czy wymianę danych w ramach funkcjonowania wszelkich komunikatorów internetowych.

W każdym z powyższych przypadków bez znaczenia pozostaje format danych, w jakim przetwarzany jest materiał pornograficzny, jak również to, czy dla jego odtworzenia niezbędne jest posiadanie szczególnych narzędzi informatycznych (np. określonego programu odtwarzającego filmy, czy też stosownego *kodeku*[143]). Analogicznie, ukrycie prawdziwego

---

[139] W ten właśnie sposób pojęcie *pozyskiwania* rozumiane jest na gruncie pkt 97 Raportu Wyjaśniającego do Konwencji. *Explanatory Report*, pełen tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[140] Pkt 96 Raportu Wyjaśniającego.

[141] B. Kunicka-Michalska, Pornografia i wykorzystywanie nieletnich w Internecie. Regulacje polskiego Kodeksu karnego, Studia Prawnicze, Zeszyt 4 (166) 2005 r., Instytut Nauk Prawnych PAN, Warszawa 2006, s. 83.

[142] Również pkt 96 Raportu Wyjaśniającego.

[143] Z ang. *codec* - program lub element programu, niezbędny do odtwarzania danych zapisanych w określonym formacie (np. kodek filmowych plików DVIX). Więcej na stronie internetowej pod adresem:

charakteru materiałów poprzez ich zaszyfrowanie nie przekreśla faktycznego wystąpienia przesłanki „posiadania”, „pobierania”, czy też „przesyłania” pornografii z udziałem dzieci, o ile tylko dany czyn został popełniony umyślnie - to jest w szczególności przy świadomości sprawcy, co do rzeczywistej treści przetwarzanego, np. ściąganego z sieci, zasobu komputerowego.

Obok opisanych wyżej regulacji Konwencji budapesztańskiej, przepisy kierowane specyficznie przeciwko rozpowszechnianiu pornografii dziecięcej w cyberprzestrzeni, obecne są także na gruncie prawodawstwa Unii Europejskiej, m. in. w dyrektywie Parlamentu Europejskiego i Rady 2011/93/EU z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej[144]. Wskazana dyrektywa zastąpiła wcześniejszą decyzję ramową Rady 2004/68/WSiSW. W ramach analizy dyrektywy w kontekście zwalczania cyberprzestępczości, konieczne jest w szczególności odniesienie się do jej dwóch przepisów, zawartych w art. 5 oraz 25:

„Artykuł 5 Przestępstwa związane z pornografią dziecięcą

1. Państwa członkowskie podejmują środki niezbędne do zapewnienia karalności czynów umyślnych, o których mowa w ust. 2–6, gdy są to czyny bezprawne.

2. Nabywanie lub posiadanie pornografii dziecięcej podlega sankcji karnej w maksymalnym wymiarze co najmniej roku pozbawienia wolności.

3. Świadome uzyskiwanie dostępu, za pośrednictwem technologii informacyjno-komunikacyjnych, do pornografii dziecięcej, podlega sankcji karnej w maksymalnym wymiarze co najmniej roku pozbawienia wolności.

4. Dystrybucja, rozpowszechnianie lub przesyłanie pornografii dziecięcej podlega sankcji karnej w maksymalnym wymiarze co najmniej dwóch lat pozbawienia wolności.

5. Oferowanie, dostarczanie lub udostępnianie pornografii dziecięcej podlega sankcji karnej w maksymalnym wymiarze co najmniej dwóch lat pozbawienia wolności.

6. Produkcja pornografii dziecięcej podlega sankcji karnej w maksymalnym wymiarze co najmniej trzech lat pozbawienia wolności.

7. Do państw członkowskich należy decyzja, czy niniejszy artykuł ma zastosowanie do przypadków związanych z pornografią dziecięcą, o których mowa w art. 2 lit. c) ppkt

---

http://pl.wikipedia.org/wiki/Kodek.

[144] Pełny tekst dyrektywy w języku polskim dostępny jest na stronie internetowej pod adresem: http://eur-lex.europa.eu/Notice.do?val=628922:cs&lang=pl&list=693607:cs,650364:cs,646021:cs,645662:cs,629114:cs,628922:cs,578961:cs,560069:cs,541735:cs,525713:cs,&pos=6&page=1&nbl=47&pgs=10&hwords=&checktexte=checkbox&visu=#texte. Dyrektywa oryginalnie została oznaczona błędnie, jako dyrektywa 2011/92/EU (92 zamiast 93). Wskazany błąd stał się przedmiotem urzędowego sprostowania.

(iii), w których osoba wyglądająca jak dziecko w momencie przedstawienia miała w rzeczywistości 18 lat lub więcej.

8. Do państw członkowskich należy decyzja, czy ust. 2 i 6 niniejszego artykułu mają zastosowanie do przypadków, w których ustalono, że materiał pornograficzny w rozumieniu art. 2 lit. c) ppkt (iv) został wyprodukowany przez producenta i znajduje się w jego posiadaniu wyłącznie do prywatnego użytku, w zakresie, w jakim do celów jego wyprodukowania nie został wykorzystany materiał pornograficzny, o którym mowa w art. 2 lit. c) ppkt (i), (ii) lub (iii), i pod warunkiem że z czynem tym nie wiąże się żadne ryzyko rozpowszechnienia danego materiału.

Artykuł 25. Środki wymierzone przeciwko stronom internetowym zawierającym lub rozpowszechniającym pornografię dziecięcą

1. Państwa członkowskie podejmują środki niezbędne do zapewnienia szybkiego usunięcia stron internetowych zawierających lub rozpowszechniających pornografię dziecięcą utrzymywanych na ich terytorium oraz by dążyć do zapewnienia usunięcia takich stron utrzymywanych poza ich terytorium.

2. Państwa członkowskie mogą podejmować środki służące blokowaniu stron internetowych zawierających lub rozpowszechniających pornografię dziecięcą wśród użytkowników internetu na swym terytorium. Środki te muszą być wprowadzone w oparciu o przejrzystą procedurę i dostarczać odpowiednich gwarancji, w szczególności w celu zapewnienia ograniczenia blokowania do tego, co konieczne i współmierne, oraz informowania użytkowników o powodzie takiego blokowania. Gwarancje te mogą również obejmować możliwość uzyskania zadośćuczynienia sądowego.”.

Zgodnie z art. 5 dyrektywy, państwa członkowskie Unii Europejskiej zostały zobowiązane do wprowadzenia karalności czynów polegających na:

- nabywaniu lub posiadaniu pornografii dziecięcej,
- świadomym uzyskiwaniu dostępu do pornografii dziecięcej za pośrednictwem „technologii informacyjno-komunikacyjnych” - termin ten, choć niezdefiniowany w dyrektywie, w preambule dokumentu odniesiony został w szczególności do wszelkich zasobów cyberprzestrzeni,
- dystrybuowaniu, rozpowszechnianiu lub przesyłaniu pornografii dziecięcej, oraz,
- oferowaniu, dostarczaniu lub udostępnianiu pornografii dziecięcej.

Pomimo wprowadzenia odwołania do „technologii informacyjno-komunikacyjnych" wyłącznie do znamienia „uzyskiwania dostępu do pornografii dziecięcej", wszystkie wymienione zachowania mogą być dokonywane w obszarze cyberprzestrzeni, mając za przedmiot wykonawczy zapis pornografii dziecięcej wyrażony w postaci danych komputerowych.

Odnosząc analizowany przepis art. 5 do zwalczania zjawiska propagacji pornografii dziecięcej w cyberprzestrzeni, należy stwierdzić, że podobnie, jak w przypadku postanowień Konwencji o cyberprzestępczości, wyliczony w nim katalog penalizowanych czynności należy odczytywać, jako kompletny, obejmujący wszelkie formy technicznego przetwarzania danych w systemach teleinformatycznych. Zgodnie z przyjętą redakcją przepisu karane jest zatem nie tylko zwykłe posiadanie materiałów pornograficznych - bez względu na ich formę (np. format pliku), rodzaj zastosowanego nośnika, czy jego dokładną lokalizację (dysk sieciowy, dane przetwarzane w chmurze, itd.), ale także wszelkie przejawy transmitowania pornografii dziecięcej poprzez sieci - w tym pobieranie materiałów ze stron, czy też ich odtwarzanie *on-line* w technologii strumieniowania danych (przesłanka „uzyskiwanie dostępu"), wysyłanie materiałów do osób trzecich, zarówno w kręgu osób ściśle oznaczonych (przesłanka „przesyłanie"), jak i nieoznaczonych (przesłanki „dystrybucja" oraz „rozpowszechnianie") i wreszcie udostępnianie materiałów w miejscu otwartym dla innych - np. na forum internetowym (przesłanka „udostępnianie").

Przytoczony art. 25 dyrektywy, choć nie przewiduje karalności określonych czynów, wprowadza szczególne regulacje mające na celu aktywne zwalczanie propagacji pornografii dziecięcej w cyberprzestrzeni. Zgodnie z tym przepisem, państwa członkowskie Unii Europejskiej zobligowane są do wprowadzenia środków prawnych oraz faktycznych niezbędnych do usuwania lub też ewentualnie blokowania, stron internetowych zawierających pornografię z udziałem dzieci. O ile obrany kierunek regulacyjny zasługuje na pełną aprobatę, o tyle wprowadzenie do redakcji przepisu wyrażenia „strona internetowa" uznać należy za niefortunny wybór, bowiem ogromne ilości zasobów Internetu nie są dystrybuowane za pośrednictwem stron lecz w technologii *peer-to-peer*, czy też w ramach sieci *torrent* - obydwie technologie opisywane były we wcześniejszych częściach pracy.

Mając za tło zaprezentowane wyżej regulacje Konwencji o cyberprzestępczości oraz dyrektywy 2011/93/EU, polska ustawa karna dokonuje typizacji czynu rozpowszechniania pornografii dziecięcej w art. 202 § 3 oraz 4a i 4b Kodeku karnego. Poniżej brzmienie przywołanych jednostek redakcyjnych:

„§ 3. Kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, przechowuje

lub posiada albo rozpowszechnia lub prezentuje treści pornograficzne z udziałem małoletniego albo treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, podlega karze pozbawienia wolności od lat 2 do lat 12.

§ 4a. Kto przechowuje, posiada lub uzyskuje dostęp do treści pornograficznych z udziałem małoletniego, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4b. Kto produkuje, rozpowszechnia, prezentuje, przechowuje lub posiada treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.”.

Zestawiając powyższe przepisy w jednolitą normę prawną ukierunkowaną na zwalczanie propagacji pornografii z udziałem małoletniego w cyberprzestrzeni, należy zauważyć, że na gruncie polskiej ustawy karnej wprowadzona została karalność czynów wypełniających następujące znamiona przestępcze:

- produkcja, utrwalanie, sprowadzanie, przechowywanie lub posiadanie treści pornograficznych z udziałem małoletniego - dokonywane w celu ich rozpowszechniania (§ 3 *in principio*).
- przechowywanie, posiadanie lub uzyskiwanie dostępu do treści pornograficznych z udziałem małoletniego poniżej lat 15 (§ 4a) - w tym wypadku bez dookreślania celu w postaci rozpowszechniania,
- rozpowszechnianie lub prezentowanie treści pornograficznych z udziałem małoletniego (§ 3 *in fine*), oraz,
- produkcja, rozpowszechnianie, prezentacja, przechowywanie lub posiadanie treści pornograficznych przedstawiających wytworzony albo przetworzony wizerunek[145] małoletniego uczestniczącego w czynności seksualnej (§ 4b).

Na marginesie warto zauważyć, że wobec braku w przepisach Kodeksu karnego definicji pojęcia „małoletni”, wyrażenie to rozumiane jest w sposób ustalony na gruncie Kodeksu cywilnego. Tym samym, małoletnim jest osoba poniżej 18 roku życia, która nie zawarła związku małżeńskiego (art. 10 § 2 Kodeksu cywilnego).

W odróżnieniu od wskazanych powyżej regulacji Konwencji o cyberprzestępczości, żaden z przytoczonych przepisów Kodeksu karnego nie otrzymał brzmienia odnoszącego się bezpośrednio do szeroko rozumianego przetwarzania, a w tym rozpowszechniania, materiałów pornograficznych z udziałem małoletniego przy zastosowaniu systemów

[145] Kategoria obejmuje w szczególności tzw. *pornografię wirtualną*, por. M. Siwicki, op. cit., s. 184.

teleinformatycznych (czy też szerzej - zasobów cyberprzestrzeni)[146]. W efekcie, na gruncie ustawy krajowej, karalność posiadania oraz propagacji materiałów pornograficznych z udziałem małoletniego - zapisanych w postaci elektronicznej, oparta została na szerokim zakresie przedmiotowym samego pojęcia „materiału", jak również zakresów semantycznych przesłanek „utrwalanie", „przechowywanie", „posiadanie", czy też „uzyskiwanie dostępu" odnoszących się do wszelkich materiałów, niezależnie od ich formy oraz postaci. O ile przyjęta konstrukcja legislacyjna zapewnia wysoki poziom elastyczności wprowadzonej regulacji karnej (ścisłe określenie form, w jakich występuje zabroniony materiał może w przyszłości okazać się nadmiernie zawężające), o tyle pominięcie w przepisie przesłanek odnoszących się specyficznie do cyberprzestrzeni uznać należy za błąd ustawodawcy[147]. W szczególności wskazać należy na nieuzasadnione pominięcie w przepisach krajowych przesłanek *przesyłania*, *pozyskiwania* oraz *oferowania lub czynienia dostępnymi* materiałów pornograficznych z udziałem nieletniego, które to przesłanki zapisane zostały wprost w regulacjach Konwencji o cyberprzestępczości. Wskazane przesłanki pozwalają nie tylko na skuteczne ściganie autorów stron internetowych zawierających zabronione materiały pornograficzne - to jest bez konieczności niezwykle trudnego w praktyce wykazywania, że oferowane materiały zostały rzeczywiście pobrane przez osoby trzecie - a tym samym zostały rozpowszechnione, ale również ich odbiorców, którzy po pobraniu określonego materiału mogą zapisać uzyskany materiał bezpośrednio na zewnętrznym nośniku danych utrudniając lub wręcz uniemożliwiając potwierdzenie wystąpienia przesłanki *posiadania* lub też *uzyskania dostępu do* materiału pornograficznego z udziałem małoletniego. W kontekście prowadzonych rozważań, na negatywną ocenę zasługuje także konstrukcja niezdefiniowanej oraz nieznanej przesłanki „sprowadzania" materiałów pornograficznych, która to przesłanka nawiązuje swoim brzmieniem do importowania określonych zasobów spoza granic kraju. O ile zatem pobieranie materiałów pornograficznych z udziałem małoletniego ze strony internetowej *hostowanej* na zagranicznym serwerze winno być oceniane, jako „sprowadzanie" materiałów, o tyle kwalifikacja pobrania treści z serwera *ftp* udostępnionego w kraju staje się niemożliwa z uwagi na brak ustawowej definicji zastosowanego pojęcia. Wątpliwości tego typu nie powinny mieć miejsca w żadnym przepisie karnym, jednak ich pojawianie się na gruncie regulacji chroniących małoletnich wydaje się szczególnie karygodne. Jako wniosek *de lege ferenda* wskazać należy na zasadność dostosowania regulacji krajowych do przyjętych

---

146 B. Kunicka-Michalska, op. cit., s. 88.

147 Cyberprzestrzeń stanowi dziś największe medium dystrybucji pornografii dziecięcej. Więcej informacji o rosnącej skali zjawiska na stronie internetowej amerykańskiego Federalnego Biura Śledczego (*FBI*), dostępnej pod adresem: http://www.fbi.gov/stats-services/publications/innocent-images-1.

rozwiązań międzynarodowych, zapewniających wyższy poziom ochrony małoletnich w cyberprzestrzeni.

Jako osobną uwagę krytyczną należy także zawrzeć odniesienie do przesłanki „uzyskania dostępu do treści pornograficznych z udziałem małoletniego" wymienionej *expressis verbis* w przepisie art. 202 § 4a Kodeksu karnego. Przesłanka te, wymagając z jednej strony przeprowadzenia trudnego dowodowo potwierdzenia, iż sprawca określonego czynu rzeczywiście uzyskał faktyczny dostęp do materiału prawnie zabronionego (co wydaje się wykraczać poza zwykłe stwierdzenie, iż sprawca „pobrał" z sieci dany materiał), z drugiej strony - z uwagi na swój obiektywny charakter, może stać się podstawą do oskarżenia o popełnienie definiowanego w tym przepisie czynu osoby, która nawet nie tyle została wprowadzona w błąd, w efekcie którego pozyskała dany plik (np. poprzez nakłonienie do kliknięcia mylnie oznaczonego odsyłacza internetowego), co wręcz osoby, której np. umyślnie wysłano na jej skrzynkę poczty internetowej materiały zawierające zabronione prawem treści pornograficzne. W takim bowiem przypadku, zachowanie polegające na otwarciu spreparowanej wiadomości, wypełnia znamię „uzyskania dostępu do treści", choć oczywiście nie może być kwalifikowane, jako działanie noszące realny zamiar zapoznania się z materiałem zawierającym pornografię z udziałem małoletniego. Potwierdzenie jednak braku takiego zamiaru może w praktyce napotykać na te same trudności, co wykazanie zamiaru pozytywnego po stronie faktycznego sprawcy przestępstwa dokonywane przez organy wymiaru sprawiedliwości (kwestie dowodzenia winy). Komentowana przesłanka dla zachowania precyzji zapisu prawnego winna zatem zostać wprost ograniczona do przypadków uzyskania dostępu do materiału pornograficznego z faktycznym zamiarem zapoznania się z nim, to jest przy wyłączeniu przypadków dostępu niezamierzonego lub wręcz sprowokowanego w sposób podstępny.

Komentowana wyżej regulacja prawna polskiego Kodeksu karnego jest ponadto uzupełniana przepisem art. 200a. Choć przepis ten nie wprowadza szczególnej karalności propagacji treści pornograficznych za pośrednictwem sieci teleinformatycznych, w swojej hipotezie przywołana jednostka redakcyjna odnosi się do pokrewnej kategorii czynów bezprawnych związanych z nawiązywaniem kontaktów z małoletnim poprzez sieć celem popełnienia przestępstwa na tle seksualnym lub też produkcji treści pornograficznych. Komentowany przepis przyjmuje następujące brzmienie:

„Art. 200a § 1. Kto w celu popełnienia przestępstwa określonego w art. 197 § 3 pkt 2 lub art. 200, jak również produkowania lub utrwalania treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje

kontakt z małoletnim poniżej lat 15, zmierzając za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalania treści pornograficznych, i zmierza do jej realizacji, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.”

Porównując cytowany wyżej przepis z komentowanym wcześniej art. 202 § 3, 4a i 4b, stwierdzić należy, iż przepis ten obejmuje swoim zakresem przedmiotowym czyn polegający na rozsyłaniu za pośrednictwem sieci treści o zupełnie innym charakterze, bowiem nie tyle stanowiących samą pornografię, co zawierających komunikaty zmierzające do sprowokowania wystąpienia czynności o charakterze seksualnym z udziałem małoletniego. Cytowany przepis dokonuje w efekcie penalizacji wszelkich działań o charakterze pedofilskim zmierzających do znalezienia ofiary napaści seksualnej lub też nakłonienia jej do poddania się czynnościom seksualnym z wyzyskaniem błędu lub też nieumiejętności do należytego pojmowania sytuacji. Należy jednocześnie podkreślić, iż zgodnie z redakcją § 1 karalne jest obecnie już samo nawiązywanie kontaktu z małoletnim zmierzające do spotkania się z nim celem popełnienia przestępstw na tle seksualnym, co wyklucza konieczność faktycznego wystąpienia tychże przestępstw, o ile tylko wykazany zostanie określony zamiar sprawcy. W § 2 przepisu ujęta została natomiast karalność składania propozycji obcowania płciowego lub poddania się innej czynności seksualnej, bądź też produkcji lub utrwalania treści pornograficznych, jednak w tym przypadku - wyłącznie przy spełnieniu dodatkowej przesłanki *zmierzania przez sprawcę do rzeczywistej realizacji* tak identyfikowanych czynności. Ten ostatni wymóg wydaje się wprowadzać istotne utrudnienie dowodowe wobec działań sprawcy, które już same w sobie - polegające przecież na namawianiu małoletniego do obcowania płciowego, winny podlegać karze niezależnie od faktu, czy sprawca będzie dalej, konsekwentnie zmierzał do realizacji proponowanych czynności. W tym kontekście wymóg ten winien zostać usunięty z przepisu. Pomimo wskazanego rozwiązania prawnego, dodanie analizowanego przepisu należy oceniać z pełną aprobatą, jako wychodzące naprzeciw rzeczywistym potrzebom organów ścigania, spotykających się coraz częściej ze zjawiskiem wykorzystywania sieci, jako kanału komunikacyjnego dla pedofilów.

Zamieszczanie w cyberprzestrzeni nielegalnych kopii programów komputerowych

Biorąc pod uwagę skalę różnych zjawisk przestępczych, prawdziwą plagą cyberprzestrzeni stało się wykorzystywanie możliwości Internetu do rozpowszechniania nielegalnych, tzw. pirackich, kopii utworów chronionych prawem autorskim. Twierdzenie to dotyczy w szczególności piractwa programów komputerowych, w tym gier, jak również utworów audio-wizualnych dostępnych w formatach cyfrowych (głównie albumy muzyczne oraz filmy). Przybliżając nieco rzeczywiste wymiary zjawiska piractwa programów komputerowych, według szacunków, w każdej chwili w sieci prowadzonych jest około 30 tysięcy aktywnych pobrań nielegalnych kopii najpopularniejszych systemów operacyjnych, zaś samo oprogramowanie firmy Microsoft pobierane jest nielegalnie przez ponad 40 tysięcy użytkowników w każdym czasie[148]. Przedstawianą skalę piractwa należy w największej mierze tłumaczyć łatwością wykonywania nielegalnych kopii materiałów przetwarzanych w systemach teleinformatycznych[149]. Samo określenie „piractwo komputerowe" stanowi nawiązanie nie tyle do piratów morskich, co przyjętego jeszcze w XVII wieku - a więc na długo przed powstaniem współczesnego prawa autorskiego, rozumienia tego wyrażenia, jako określającego wszelkiego rodzaju naruszenia własności intelektualnej[150]. Ponownie, z uwagi na specjalistyczny charakter pracy, niniejsza analiza skupia się wyłącznie na kwestiach szczególnych dla zwalczania naruszeń prawa autorskiego w cyberprzestrzeni, pozostawiając analizę kwalifikacji oraz ścigania naruszeń własności intelektualnej w ogóle.

Z punktu widzenia technicznego, cyberprzestrzeń tworzy liczne możliwości dla naruszeń praw autorskich, które to naruszenia mogą wyrażać się w wielu zróżnicowanych czynach. O ile mówiąc o „piractwie komputerowym" najczęściej ma się na myśli wykonywanie nielegalnych kopii oprogramowania komputerowego lub też utworów audio-wizualnych, o tyle w rzeczywistości taka działalność stanowi jedynie fragment opisu zjawiska.

Zgodnie z przyjętymi globalnie standardami prawnymi, naruszeniem praw autorskich jest każde nieuprawnione wykorzystanie dowolnego utworu podlegającego ochronie. W cyberprzestrzeni, efekt ten może zostać osiągnięty wobec chronionego programu w szczególności poprzez[151]:

---

[148] Tak np. wyniki badań Starmedia zamieszczone na stronie internetowej dostępnej pod adresem: https://torrentfreak.com/software-piracy-110822/

[149] M. Siwicki, op. cit., s. 259.

[150] Tak np. na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Copyright_infringement.

[151] Klasyfikacja częściowo oparta na: B. Fischer, op. cit., s. 72 i nast.

1) wykonywanie nielegalnych (w szczególności niezgodnych z udzieloną licencją) kopii oprogramowania - zarówno kodu skompilowanego, to jest zapisanego w postaci wykonywalnej, jak również tzw. kodu źródłowego, wymagającego odpowiedniego przetworzenia. Nielegalne tworzenie kopii obejmuje powielanie zarówno plików instalacyjnych, jak również plików już zainstalowanych na komputerze. Dla oceny kopii, jako bezprawnej, bez znaczenia pozostaje fakt, czy kopia wykonywana jest za pośrednictwem sieci (to jest czy powielane dane są uprzednio transmitowane przez sieć), czy też lokalnie (na pojedynczym komputerze), jak również rodzaj zastosowanego nośnika oryginału oraz kopii (optyczny - CD, DVD, BD, magnetyczny - dysk twardy, pamięci półprzewodnikowe - *flash*, SSD, itd). Z pojęcia nielegalnych kopii wyłączone są tzw. kopie zapasowe programów, wykonywane na użytek osoby legalnie dysponującej danym programem;
2) łamanie lub omijanie zabezpieczeń programów (np. kluczy, numerów seryjnych, czy też aktywacji sieciowych), które to zabezpieczenia ograniczają bądź też całkowicie uniemożliwiają wykorzystywanie funkcji oprogramowania. Warto nadmienić, że wiele programów jest aktualnie dystrybuowanych wyłącznie za pośrednictwem sieci, zaś samo ich pobranie jest zupełnie legalne oraz bezpłatne. Możliwość skorzystania z takiego oprogramowania wiąże się jednak z koniecznością wniesienia opłaty licencyjnej na rzecz jego producenta oraz wprowadzenia w programie odpowiedniego kodu odblokowującego określoną licencję użytkownika końcowego. Nierzadko programy udostępniane są dziś w sieci w tzw. wersji ewaluacyjnej, np. ograniczonej w czasie działania do 30 dni (wersje *trial*);
3) tworzenie oraz dystrybuowanie specjalistycznych narzędzi służących do łamania zabezpieczeń programów (np. generatorów kluczy, tzw. *keygen*) oraz wszelkich powielania utworów zapisanych w postaci cyfrowej;
4) wykorzystywanie dowolnego utworu, w tym zarówno programu komputerowego, jak i utworu audio-wizualnego, niezgodnie z zasadami udzielonej licencji, np. poprzez jego udostępnienie zbyt wysokiej liczbie użytkowników, czy też niedozwolone upublicznienie nagrania w Internecie (w tym także rozpowszechnianie w sieci odkodowanego sygnału telewizyjnego);
5) uzyskiwanie nieuprawnionego dostępu do programu komputerowego lub innego utworu zapisanego w postaci cyfrowej, poprzez przełamanie lub ominięcie zabezpieczeń określonej usługi sieciowej, np. włamanie się do Internetowej

wypożyczalni filmów, czy zalogowanie się do sieciowego serwisu oferującego określone utwory, z wykorzystaniem spreparowanych loginów oraz haseł;

6) wprowadzanie nieuprawnionych modyfikacji w oprogramowaniu komputerowym mogących służyć zarówno łamaniu lub omijaniu zabezpieczeń, zmianie licencji przypisanej do programu (np. zmiana wersji systemu operacyjnego z domowej na profesjonalną), jak również modyfikacjom funkcjonalności oprogramowania.

Powyższy katalog, pomimo swojego rozbudowania wymienia jedynie najbardziej typowe przejawy naruszeń praw autorskich do programu komputerowego w cyberprzestrzeni. Ostatecznie, warto też zauważyć, że wraz z rozwojem cyberprzestrzeni oraz pojawianiem się nowych usług sieciowych liczba możliwości naruszeń praw autorskich ustawicznie wzrasta (np. pojawienie się tzw. telewizji internetowej oraz usługi filmów na żądanie - VOD).

Przenosząc dalsze rozważania na grunt prawniczy, powyższa lista naruszeń pozwala na postawienie dwóch tez: po pierwsze, jak istotne dla zapewnienia skutecznej ochrony praw autorskich w cyberprzestrzeni jest stworzenie specyficznych regulacji prawnych, odnoszących się do ochrony własności intelektualnej w obszarze domeny cyfrowej, oraz po drugie - jak szeroki powinien być zakres takich regulacji. Z uwagi na globalny zasięg cyberprzestrzeni, zwalczanie naruszeń praw autorskich w jej obszarze musi zapewniać także skuteczną współpracę międzynarodową opartą na jednoznacznym ustaleniu jurysdykcji poszczególnych państw.

Na poziomie prawa międzynarodowego, jako przykład regulacji nakierowywanych na prawno-karne zwalczanie naruszeń praw autorskich w cyberprzestrzeni - w tym naruszeń praw do programu komputerowego, wskazać należy w szczególności na postanowienia Konwencji Rady Europy o cyberprzestępczości. Zgodnie z art. 10 Konwencji, zatytułowanym „Przestępstwa związane z naruszeniami praw autorskich oraz praw pokrewnych":

1. Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego naruszenia praw autorskich, rozumianego w sposób zdefiniowany przez tę Stronę w jej prawie, zgodnie ze zobowiązaniami przyjętymi na gruncie Aktu Paryskiego z dnia 24 lipca 1971 r. zmieniającego Konwencję Berneńską o Ochronie Dzieł Literackich oraz Artystycznych, Porozumienia w sprawie Handlowych Aspektów Praw Własności Intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o Prawach Autorskich, z wyłączeniem wszelkich praw moralnych przytaczanych przez te akty, o ile takie naruszenia popełniane są rozmyślnie, na skalę komercyjną oraz

z zastosowaniem systemu komputerowego.

2. Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego naruszenia praw pokrewnych, rozumianego w sposób zdefiniowany przez tę Stronę w jej prawie, zgodnie ze zobowiązaniami przyjętymi na gruncie Międzynarodowej Konwencji o Ochronie Wykonawców, Producentów Fonogramów i Organizacji Nadawczych (Konwencja Rzymska), Porozumienia w sprawie Handlowych Aspektów Praw Własności Intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o Wykonaniach i Fonogramach, z wyłączeniem wszelkich praw moralnych przytaczanych przez te akty, o ile takie naruszenia popełniane są rozmyślnie, na skalę komercyjną oraz z zastosowaniem systemu komputerowego.

3. Każda ze Stron może zastrzec prawo do wyłączenia odpowiedzialności karnej, o której mowa w ust. 1 i 2 niniejszego artykułu w określonych przypadkach, o ile dostępne są inne skuteczne środki prawne, zaś takie zastrzeżenie nie wyłącza realizacji zobowiązań Strony wynikających z instrumentów, o których mowa w ust. 1 i 2 niniejszego artykułu."[152].

Komentując powyższy przepis, nie sposób nie podnieść, iż pomimo specjalistycznego charakteru konwencji, nastawiającego cały akt na zwalczanie specyficznych przejawów przestępczości komputerowej, przytoczony przepis zachowuje wysoce ogólny charakter, pomijając wszelkie szczególne aspekty związane z przetwarzaniem danych komputerowych w cyberprzestrzeni. W istocie, jedynym zawartym w przepisie odniesieniem do domeny cyfrowej pozostaje przywołanie na końcu analizowanej jednostki redakcyjnej wyrażenia „system komputerowy", pozwalającego odnieść wszelkie naruszenia praw autorskich opisane

[152] Art. 10 Konwencji o cyberprzestępczości. W oryginale: „*Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.*". Tłumaczenie własne.

w przytoczonych aktach międzynarodowych, także do naruszeń popełnionych w ramach pracy w systemie komputerowym. Innymi słowy, istotą regulacji Konwencji o cyberprzestępczości w zakresie ochrony praw autorskich w obszarze cyberprzestrzeni, stało się wprowadzenie zasady uznawania za przestępstwo wszelkich naruszeń praw autorskich odnoszących się do danych komputerowych, których bezprawność wynika z przywołanych w przepisie, juz obowiązujących regulacji prawnych. Zgodnie z Konwencją, aby naruszenia takie mogły być uznawane za przestępstwo, muszą być jednak popełniane „rozmyślnie" oraz „na skalę komercyjną".

Przenosząc się na grunt prawodawstwa Unii Europejskiej, w ramach którego wykształcony został rozległy system ochrony prawa autorskiego, jednym z podstawowych, aktualnych aktów normatywnych ustanawiających ramy dla prawno-autorskiej ochrony programów komputerowych, jest dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych[153]. Choć dyrektywa nie wprowadziła obowiązku penalizacji poszczególnych naruszeń praw autorskich do programu komputerowego, poprzez określenie zakresu ochrony tych praw, wyznaczyła jednak obszar działań bezprawnych, nakładając jednocześnie na państwa obowiązek wprowadzenia stosownych środków prawnych mających na celu ochronę twórcy oraz legalnego użytkownika oprogramowania. W szczególności, dyrektywa określiła w art. 7 ust. 1 lit. a - c bezprawność trzech, następujących kategorii działań:

1) wprowadzanie do obrotu kopii programu komputerowego, jeśli dana osoba wiedziała lub miała podstawy do przyjęcia, że czynność dotyczy tzw. kopii nielegalnej;
2) posiadanie do celów komercyjnych kopii programu komputerowego, jeśli dana osoba wiedziała lub miała podstawy do przyjęcia, że jest to kopia nielegalna; oraz,
3) wprowadzanie do obrotu lub posiadanie do celów komercyjnych wszelkich środków, których jedynym przeznaczeniem jest ułatwienie niedozwolonego usuwania lub obchodzenia jakichkolwiek urządzeń technicznych, które mogłyby zostać zastosowane do ochrony programu komputerowego.

W oparciu o tak zakreślone międzynarodowe ramy prawne (ich szczegółowe przybliżenie dalece wykracza poza cel i ramy niniejszego rozdziału, stanowiąc w istocie temat dla obszernej pracy doktorskiej), polski ustawodawca wprowadził do krajowego porządku prawnego szereg regulacji mających na celu ochronę praw autorskich do programów

---

[153] Pełny tekst dyrektywy w języku polskim dostępny jest na stronie internetowej pod adresem: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:PL:PDF.

komputerowych, zawierających się w szczególności w Kodeksie karnym oraz ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[154]. Z uwagi na rozległość przedstawianego zagadnienia, dalsza analiza prawna ograniczona zostaje do regulacji penalizujących nielegalne udostępnianie oraz nielegalne pobieranie programów komputerowych.

Poniżej brzmienie przepisu art. 116 przywołanej ustawy o prawie autorskim i prawach pokrewnych:

> Art. 116. 1. Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
>
> 2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności do lat 3.
>
> 3. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od 6 miesięcy do lat 5.
>
> 4. Jeżeli sprawca czynu określonego w ust. 1 działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Przytoczony przepis obejmuje programy komputerowe poprzez ogólne określenie ochrony dla utworów, w których skład wchodzą także programy. Zastosowane w ust. 1 sformułowanie „bez uprawnienia albo wbrew jego warunkom" należy odczytywać, jako odesłanie do ogólnych zasad prawa autorskiego oraz umów licencyjnych określających zasady użytkowania (w tym tzw. pola eksploatacji programu komputerowego) oraz rozpowszechniania określonego programu. W konsekwencji, zgodnie z art. 116 ust. 1 prawa autorskiego, na mocy przywołanego przepisu karane jest nie tyle wykonywanie ściśle określonych czynności, ale każde zachowanie naruszające uprawnienia właściciela autorskich praw majątkowych do programu, wykraczające jednocześnie poza zakres upoważnienia do korzystania z programu udzielonego jego użytkownikowi końcowemu w ramach licencji. Warto także zaznaczyć, że ustawa nie definiuje określenia „cudzy utwór", domyślnie rozumiejąc pod pojęciem tym utwór stworzony przez inna osobę.

Zgodnie z art. 278 § 2 w zw. z § 1 Kodeksu karnego:

> „Art. 278. § 1. Kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą, podlega karze

[154] Dz. U. z 2006, Nr 90, poz. 631, z późn. zm.

pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej.”.

Faktyczne zaistnienie przestępstwa stypizowanego w § 2 wymaga łącznego spełnienia przez określony czyn trzech przesłanek:

- „uzyskania” przez sprawcę cudzego programu komputerowego,
- uzyskanie programu musi nastąpić bez zgody osoby uprawnionej,
- działanie sprawcy musi być nakierowane na uzyskanie korzyści majątkowej.

Wymienione przesłanki ocenić należy jako nieprecyzyjne oraz budzące szereg wątpliwości interpretacyjnych.

Po pierwsze, zacytowany przepis Kodeksu karnego penalizuje wyłącznie czyn polegający na aktywnym uzyskiwaniu programu, a więc pomija kwestie karalności jego dystrybucji, które zawarte zostały w ustawie o prawie autorskim i prawach pokrewnych[155].

Po drugiej, samo sformułowanie znamienia wykonawczego przestępstwa, ujęte w redakcji przepisu, jako „uzyskiwanie”, jest wysoce niejasne. Mając na uwadze przedstawiony na wstępie analizy katalog przykładowych czynności technicznych, konstytuujących naruszenia praw autorskich w cyberprzestrzeni, faktyczne „uzyskanie” programu może nastąpić zarówno przez jego bezprawne pobranie z sieci, czy powielenie, jak również przełamanie zabezpieczeń chroniących dostęp do programu lub ograniczających bądź też wyłączających jego funkcjonalność (np. przełamanie zabezpieczeń wersji *trial*, czyli wersji programu ograniczonej w działaniu czasowo, np. do 30 dni). Z uwagi na lakoniczne ujęcie przepisu, brak jest możliwości udzielenia jednoznacznej odpowiedzi na pytanie, czy znamię „uzyskiwania” obejmuje również tak charakteryzowane czynności techniczne, które *de facto* nie polegają na nielegalnym *pozyskaniu* (np. pobraniu) samego programu, lecz na jego użytkowaniu niezgodnie z zasadami określonymi przez właściciela lub uprawnionego dysponenta praw autorskich.

Po trzecie, penalizując uzyskanie „cudzego” programu „bez zgody osoby uprawnionej” przepis nie tylko nie wyjaśnia obydwu tych pojęć, ale także nie zwraca należytej uwagi na relacje, jakie mogą pomiędzy nimi zachodzić. Na gruncie Kodeksu karnego - ustawy mającej zupełnie inną rolę niż wcześniej przywołana ustawa o prawie autorskim i prawach pokrewnych, wyraz „cudzy” nie przesądza jednoznacznie, czy chodzi tu o osobę będącą właścicielem majątkowych praw autorskich do programu, czy też

[155] Por. M. Siwicki, Cyberprzestępczość, C. H. Beck, Warszawa 2013, s. 262 oraz s. 269.

o użytkownika końcowego programu, który posiada jego legalną kopię wraz ze stosowna licencją? Rozstrzygnięcie tej kwestii kształtuje w istocie brzegowy zakres karnoprawnej ochrony praw autorskich do programu, odpowiadając na pytanie - czy program spersonalizowany przez użytkownika końcowego, np. z wprowadzonymi skrótami, opisami, odpowiednio skonfigurowanymi opcjami, podlega także ochronie w kontekście wymienionych ustawień? Innymi słowy - czy wyraz „cudzy" odnosi się także do faktycznie *wykradanego* egzemplarza programu, czy też wyłącznie do programu w jego oryginalnej wersji, dystrybuowanej przez właściciela praw majątkowych. Sformułowanie „osoba uprawniona" - stanowiące proste odesłanie do zasad prawnych regulujących kwestie praw autorskich oraz ich zarządu, wprowadza z kolei zamieszanie interpretacyjne na tle zastosowania w danym przepisie dwóch różnych określeń odwołujących się do osób - tj. „cudzy" oraz „osoba uprawniona". Osobą uprawnioną do dysponowania prawami autorskimi do programu jest w pierwszej kolejności ich właściciel, a zatem, jak się wydaje, osoba kryjąca się w przepisie pod sformułowaniem „cudzy". W takiej sytuacji, wprowadzone rozróżnienie semantyczne okazuje się sztuczne, nazywając jedną osobę dwoma różnymi określeniami prawnymi.

Po czwarte, wymóg ażeby działanie sprawcy było nakierowane na uzyskanie korzyści majątkowej powoduje istotne obniżenie ochrony programów komputerowych, nakazując każdorazowo ustalać określony zamiar sprawcy przestępstwa o charakterze obiektywnym. Należy także wskazać na istotne wątpliwości co do oceny uzyskania korzyści majątkowej, w sytuacji, w której sprawca przestępstwa uzyskuje nielegalną kopię programu wyłącznie w celu jego przetestowania przed legalnym zakupem. Ustawowy wymóg wprowadza w konsekwencji niebezpieczną dawkę ocenności zachowania sprawcy analizowanego czynu.

§3. Cyberprzestępstwa związane z uzyskaniem nieuprawnionego dostępu do systemu

Trzecia z wyróżnionych kategorii cyberprzestępczości obejmuje czyny polegające na uzyskiwaniu nieuprawnionego dostępu do wnętrza systemu teleinformatycznego za pośrednictwem cyberprzestrzeni. W kształtującej się w Polsce doktrynie prawa karnego komputerowego działania takie nierzadko określane są mianem „klasycznego hackingu".

Określając podstawowe cechy cyberprzestępczości związanej z uzyskiwaniem nieuprawnionego dostępu do systemów, wyróżniające tę kategorię czynów od pozostałych odmian cyberprzestępczości, w pierwszej kolejności należy wskazać, iż o ile „wtargnięcie" do dowolnego systemu podłączonego do sieci wymaga oczywiście dokonywania transmisji danych pomiędzy systemami atakującym oraz atakowanym (już samo przejrzenie zasobów

atakowanego komputera oznacza przekazanie pomiędzy maszynami danych, np. swoistej listy zawartości systemu atakowanego), o tyle w przypadku tej formy cyberprzestępczości transmisja danych nie konstytuuje obszaru popełnienia przestępstwa, stanowiąc jedynie niezbędne medium dla faktycznego działania sprawcy (w tym kontekście, można powiedzieć, że transmisja danych stanowi w cyberprzestrzeni ekwiwalent ruchu). Jednocześnie, cyberprzestępstwa związane z uzyskiwaniem dostępu do systemu lub jego zasobów nie polegają na propagacji określonych treści lub materiałów w cyberprzestrzeni, ani dokonywaniu dalszych zmian w „otworzonym" systemie (ataki tego typu prezentowane są kolejnej części rozdziału, stanowiąc następstwo uzyskania dostępu do systemu).

Od strony technicznej, uzyskanie nieuprawnionego dostępu do systemu teleinformatycznego lub jego określonych zasobów wiąże się w szczególności z przełamaniem lub też ominięciem zabezpieczeń ograniczających ów dostęp[156], choć z prawnego punktu widzenia, za nieuprawnione należy uznawać także bezprawne poruszanie się po systemie niezabezpieczonym - o czym szerzej w dalszej części rozdziału. Jednocześnie, „dostęp do systemu", to nie tylko dostęp do zasobów zapisanych na informatycznym nośniku danych podłączonym do komputera, ale także dostęp do ustawień systemu oraz dostęp do wykonywanej przez system pracy (np. podgląd ruchu sieciowego obsługiwanego przez kartę sieciową komputera - a zatem nie podsłuch samej transmisji, a wgląd w listę aktywnych połączeń). Efekty w postaci przełamania lub ominięcia zabezpieczeń mogą zostać osiągnięte dwojako - po pierwsze, w drodze odpowiednio przygotowanego cyberataku, po drugie zaś – w ramach specyficznych czynności mających na celu określenie, a następnie wykorzystanie słabości oraz luk bezpieczeństwa danego systemu[157]. Nierzadko obydwie te metody wykorzystywane są równolegle, jako uzupełniające się narzędzia.

Do najbardziej typowych technik mających na celu uzyskanie nieuprawnionego dostępu do systemu zaliczyć można[158]:

- skanowanie atakowanego systemu w celu określenia jego podatności (tzw. *vulnerability scanning*). Sprawdzeniu poddawane są w szczególności zainstalowane na komputerze programy (wersja systemu operacyjnego, rodzaj przeglądarki internetowej, wykorzystywane oprogramowanie antywirusowe oraz tzw.

[156] Problematykę tę podkreśla S. Bukowski w: Przestępstwo hackingu, Przegląd Sądowy, Nr 4, Lexis Nexis, Warszawa 2005 r., s. 153.
[157] Np. tzw. *port scanning technic*, czyli działalnie polegające na skanowaniu portów sieciowych celem ustalenia, które z nich są otwarte. Por. M. Siwicki, op. cit., s. 96.
[158] Lista przygotowana m.in. w oparciu o zasoby dostępne na stronie internetowej pod adresem: http://en.wikipedia.org/wiki/Hacker_(computer_security)#Attacks.

zapora ogniowa), jak również porty sieciowe wykorzystywane przez atakowany system do transmisji danych,

- wykorzystywanie zidentyfikowanych podatności bezpieczeństwa - np. błędów zainstalowanego oprogramowania pozwalających ominąć wszelkie zabezpieczenia, czy też umożliwiających zmuszenie systemu do wykonania operacji poleconych „z zewnątrz", za pośrednictwem sieci (np. atak na systemy bazodanowe, tzw. SQL *injection*[159], polegający na sprowokowaniu zaatakowanego systemu do błędnego wysłania fragmentów obsługiwanej bazy danych do sprawcy), jak również błędów w konfiguracji systemów bezpieczeństwa (np. niepoprawnej konfiguracji serwera, zezwalającej nie tylko na przeglądanie zasobów danej strony internetowej, ale także ich modyfikację),
- łamanie, przejmowanie lub też wyłudzanie haseł zabezpieczających dostęp do systemu - hasła mogą być pozyskiwane zarówno w ramach specjalistycznego ataku na dany system, jak również w drodze podsłuchu transmisji danych, w której zawiera się hasło (np. atak *spoofing*, prezentowany w części 1 rozdziału - należy zauważyć, że podsłuch transmisji nierzadko stanowi etap przygotowawczy do włamania do systemu). Wyłudzenie hasła (nazywane w języku informatycznym *phishingiem*) polega na wprowadzeniu osoby znającej hasło w błąd, skutkujący jego nierozważnym udostępnieniem osobie trzeciej,
- stosowanie odpowiednio spreparowanych narzędzi oraz programów, np. wirusów, koni trojańskich, czy też tzw. robaków komputerowych, które po wprowadzeniu do komputera ofiary (infekcja najczęściej stanowi efekt niedbałości samego użytkownika, który nie stosuje podstawowych zasad bezpieczeństwa) mogą umożliwiać zdalny dostęp do systemu (w tym także przejęcie nad nim kontroli),
- stosowanie metod tzw. inżynierii społecznej, czy też szeroko rozumianego oszustwa komputerowego - analizowanego z uwagi na swoją specyfikę osobno w ostatniej części rozdziału.

Dwie pierwsze kategorie technik (to jest skanowanie systemów oraz wykorzystywanie określonych w ten sposób podatności), stanowią trzon *hackingu* w znaczeniu wąskim.

Z uwagi na powszechność występowania określonych kategorii błędów oraz

[159] W uproszczeniu, atak *SQL injection* wykorzystuje lukę bezpieczeństwa zezwalającą na wpisanie np. w polu wyszukiwarki strony, komendę, która następnie zostanie wykonana przez zaatakowany system. Więcej na temat poruszanego ataku na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/SQL_injection.

podatności systemów bezpieczeństwa, do przeprowadzania ataków cybernetycznych coraz częściej wykorzystuje się także krótkie, specjalistyczne programy komputerowe, pisane specjalnie do wykorzystania określonej słabości systemu. Programy takie, stanowiące gotowe narzędzia ataku, nazywane są *exploitami*[160]. „Niedzielnych hackerów" posługujących się nimi w toku przeprowadzania ataków, określa się z kolei mianem „*script kiddies*"[161] (sformułowanie to charakteryzuje wysoce lekceważąca konotacja).

Przenosząc dalsze rozważania na grunt prawniczy, podstawową, wręcz standardową regulacją karną penalizującą uzyskanie nieuprawnionego dostępu do systemu komputerowego, stała się norma zawarta w art. 2 Konwencji Rady Europy o cyberprzestępczości. Jak stanowi wskazany przepis:

> „Artykuł 2 - Nieuprawniony dostęp
>
> Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego, popełnionego umyślnie czynu polegającego na nieuprawnionym uzyskaniu dostępu do całości lub dowolnej części systemu komputerowego. Strona może wprowadzić wymóg zakładający karalność jedynie czynu polegającego na przełamaniu środków bezpieczeństwa, czynu popełnionego z zamiarem pozyskania danych komputerowych lub innym nieuczciwym zamiarem, lub czynu popełnionego w stosunku do systemu komputerowego połączonego z innym systemem komputerowym."[162].

Podstawowymi elementami konstytuującymi tak określone przestępstwo są w efekcie:

- wystąpienie sytuacji faktycznej „uzyskania dostępu do całości lub dowolnej części systemu", oraz,
- kwalifikacja prawna owego dostępu, jako „dostępu nieuprawnionego" oraz „zamierzonego".

Oba wskazane elementy wymagają nieco bliższej analizy.

Pojęcie „dostępu do systemu" posiada w języku informatycznym szeroką konotację[163].

---

[160] Określeniem *exploit* określa się często także gotowe instrukcje przeprowadzenia ataku. Więcej na ten temat na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Exploit_(computer_security).

[161] Por. M. Siwicki, op. cit., s. 96.

[162] Art. 2 Konwencji o cyberprzestępczości. W oryginale: „*Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*". Tłumaczenie własne. W oficjalnym przekładzie Konwencji wyrażenie „*illegal access*" zostało przetłumaczone, jako „nielegalny dostęp".

[163] Przykładowo, w języku informatycznym mówi się o „dostępie programów do pamięci". Dostęp ten oznacza

Obejmuje ono w zasadzie każdą formę „dostania się do wnętrza systemu", czyli uzyskania jakiejkolwiek kontroli nad ustawieniami, procesami lub też zasobami danego systemu. Za „dostęp do systemu" nie uznaje się czynności jedynie „odbijanych" przez system, jak np. próba wpisania błędnego hasła, czy też wysłanie do serwera komendy *ping*, pozwalającej na zmierzenie czasów reakcji pomiędzy dwoma maszynami (np. komputerem domowym a węzłem dostawcy usług internetowych). Dostępem nie jest także skanowanie portów komputera, którą to czynność przyrównać można w pewnym uproszczeniu do przyjrzenia się zamkniętym drzwiom w celu policzenia ilości zamontowanych na nich zamków - o ile działanie takie z pewnością nie wróży niczego dobrego, samo w sobie nie podlega penalizacji (porty, podobnie, jak drzwi, wystawione są na otwarty „widok" publiczny). Pojęcie „dostępu" charakteryzowane jest w Raporcie Wyjaśniającym do Konwencji, jako:

> „Pkt 46. „Dostęp" oznacza wejście do całości lub dowolnej części systemu komputerowego (zasoby sprzętowe, komponenty, przechowywane dane zainstalowanego systemu, katalogi, ruch sieciowy oraz inne dane). Jednocześnie, „dostęp" nie obejmuje prostego wysłania wiadomości e-mail, czy też pliku do systemu. Pojęcie „dostępu" obejmuje zarówno wejście do innego systemu za pośrednictwem publicznych sieci telekomunikacyjnych, jak również wejście do systemu działającego w tej samej sieci, np. sieci lokalnej lub sieci Intranetowej funkcjonującej w ramach jednej organizacji. Metoda komunikacji (np. na odległość, z użyciem łączności bezprzewodowej, czy też komunikacja bliskiego zasięgu) nie ma tu żadnego znaczenia."[164].

Co było podkreślane, dostęp do systemu nie może być ograniczany do uzyskania dostępu do samych plików nagranych na atakowanym komputerze. W szczególności, dostęp do systemu w żadnym razie nie przesądza uzyskania dostępu do jakichkolwiek informacji zapisanych na komputerze (czy to w pamięci ulotnej, czy też na trwałych, informatycznych nośnikach danych) oraz nie może być z takim dostępem do informacji utożsamiany. Zależność

---

uprawnienie programów do zapisywania oraz odczytywania pamięci. Użytkownicy uzyskują najczęściej dostęp do systemu operacyjnego (forma dopuszczenia do pracy w systemie), katalogów (forma udostępnienia określonych plików za pośrednictwem sieci), czy też urządzeń (np. możliwość drukowania materiałów na określonej drukarce). Hasło opracowane przy wykorzystaniu internetowych słowników oraz zasobów: http://www.webopedia.com/TERM/A/access.html, http://www.merriam-webster.com/dictionary/access, http://en.wikipedia.org/wiki/Filesystem_permissions oraz http://en.wikipedia.org/wiki/Access_control.

[164] Pkt 46 Raportu Wyjaśniającego do Konwencji. W oryginale: *„46. "Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. "Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.*". Tłumaczenie własne.

zachodzącą pomiędzy „uzyskaniem dostępu do systemu", a uzyskaniem „dostępu do informacji" można zarysować następująco - uzyskanie dostępu do informacji przetwarzanej wewnątrz systemu (nie zaś informacji transmitowanej, znajdującej się już w sieci!) musi wiązać się z uprzednim uzyskaniem dostępu do samego systemu.

Uzyskanie dostępu choćby do części systemu obejmuje możliwość przejęcia kontroli nad jego określoną funkcjonalnością. Wysłanie do systemu wiadomości pocztowej, czy też wiadomości kierowanej z zastosowaniem komunikatora internetowego nie konstytuuje takiego przejęcia kontroli, bowiem zostało wcześniej „przewidziane" przez uprawnionego użytkownika danego systemu oraz obsługiwane jest przez ten system w sposób zaprogramowany (innymi słowy, odebranie wiadomości jest częścią normalnej pracy systemu nie zaś wynikiem zdalnego przejęcia kontroli). Podobnie, za dostęp do systemu nie może być uznawane zamieszczanie na stronach internetowych skryptów wykonywanych po stronie komputera-odbiorcy (np. skrypty animujące elementy strony), których obsługa stanowi standardową funkcjonalność oprogramowania służącego do przeglądania stron internetowych. Dostępem do systemu jest natomiast uzyskanie kontroli nad przyłączoną do systemu kamerą internetową, uzyskanie kontroli nad drukarką, czy wreszcie przejęcie dowolnych innych peryferiów (np. klawiatury)[165].

Zastosowanie w przepisie pojęcia „nieuprawnionego dostępu" oznacza natomiast, że określony powyżej „dostęp do systemu" podlega penalizacji karnej tylko w przypadku, gdy narusza uprawnienia przysługujące wyłącznie użytkownikowi systemu. Z uwagi na brak jednoznacznych regulacji prawnych odnoszących się do zasad postępowania w cyberprzestrzeni (warto dodać – brak regulacji funkcjonujący równolegle do ustawicznego rozwoju technologicznego) rekonstrukcja katalogu takich „praw wyłącznych użytkownika" nastręcza jednak coraz więcej kłopotów. Nowe usługi sieciowe, takie jak przetwarzanie danych w chmurze (umożliwiające korzystanie z własnych danych oraz programów w dowolnym punkcie na ziemi, przy zastosowaniu dowolnego komputera, który tylko posiada łączność z Internetem), czy też wyszukiwanie spersonalizowanych zasobów (np. wyświetlanie w wyszukiwarce jedynie restauracji znajdujących się w pobliżu ustalonej lokalizacji użytkownika) coraz bardziej zacierają granicę pomiędzy tym, co pozostaje w wyłącznej gestii użytkownika, a tym, co przetwarzane jest przez dostawcę określonych usług sieciowych.

Od strony formalnej, uprawnionymi działaniami w systemie, są wyłącznie te działania,

---

[165] W tym kontekście zupełnie niezrozumiały pogląd wygłasza w swoim opracowaniu przedmiotowym M. Siwicki, uznając, że kryminalizacja przytaczanych zachowań na gruncie przepisu art. 267 § 2 Kodeksu karnego jest „paradoksalna". Tak w: M. Siwicki, op. cit., s. 116.

które bądź to zostały uprawnione na mocy stosownego przepisu (np. przepisu kompetencyjnego określonych służb), bądź też działania, na które użytkownik systemu wyraził zgodę[166] - choćby dorozumianą, wyrażoną w postaci świadomej instalacji danego programu, udzielenia programowi lub innemu użytkownikowi określonych uprawnień w systemie lub też skonfigurowanie własnego systemu w określony sposób, np. zezwalający na automatyczne pobieranie określonych treści (np. łatek systemowych), czy stosowanie wybranych technologii (np. tzw. ciasteczek[167]). Kwestia „uprawnienia" przez użytkownika musi być zatem oceniana w określonym kontekście, z zastosowaniem kryteriów obiektywnych oraz subiektywnych - to jest z odwołaniem do przyjętych praktyk oraz rzeczywistego zamiaru użytkownika. „Nieuprawnione w systemie" pozostają w konsekwencji te działania, które nie zostały dopuszczone przez osobę będącą gestorem danego systemu, w szczególności zaś działania, które zostały ukryte przed jego świadomością oraz kontrolą. Za nieuprawnione należy ponadto uznawać działania wprowadzające użytkownika w błąd - np. sprzeczne z udzieloną użytkownikowi informacją, domyślne ustawienia instalowanego programu zezwalające na wprowadzanie przez program określonych, niezakomunikowanych zmian w systemie.

Odnosząc się do znamienia bezprawności dostępu, należy wreszcie podkreślić, że brak zastosowania przez użytkownika jakichkolwiek zabezpieczeń nie może być odczytywany, jako „otwarcie" jego systemu dla wszystkich użytkowników cyberprzestrzeni[168]. Każdy system - a zatem nie tylko taki, który został należycie zabezpieczony, podlega bowiem ochronie prawnej gwarantującej prawo do prywatności, poufności oraz nienaruszalności praw i swobód człowieka i obywatela - występującego tu w roli użytkownika oraz gestora systemu komputerowego. Wejście do niezabezpieczonego systemu, które dokonywane jest bez stosownej zgody oraz wiedzy jego właściciela, musi zatem być również oceniane, jako „nieuprawnione". Warto również dodać, że aktualne regulacje prawne - zarówno międzynarodowe, jak i krajowe, nie przewidują obowiązku zabezpieczania prywatnych systemów teleinformatycznych, które nie są wykorzystywane do realizacji usług świadczonych w ramach prowadzonej działalności gospodarczej. Wszelkie wymogi w tym zakresie obejmują wyłącznie systemy przedsiębiorców telekomunikacyjnych, systemy

---

[166] Pkt 47 Raportu Wyjaśniającego do Konwencji.

[167] Pkt 48 Raportu Wyjaśniającego do Konwencji.

[168] Jak zauważa jednak M. Siwicki, w niektórych ustawodawstwach np. Austriackim, Litewskim, czy Estońskim, element przełamania zabezpieczeń stanowi jedną z przesłanek przestępności hackingu. Tak w: M. Siwicki, op. cit., s. 106 oraz przywołani tam L. Picotti, I. Salvadori, *National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices*, opracowanie dostępne na stronie internetowej Rady Europy.

przetwarzające dane kontrahentów, czy też systemy należące do teleinformatycznej infrastruktury krytycznej kraju lub systemy świadczące usługi publiczne.

Ostatecznie, karalność nieuprawnionego dostępu do systemu, została na gruncie Konwencji ograniczona do przypadków świadomego „wtargnięcia" do systemu, a zatem nie obejmuje przypadków nieumyślnego naruszenia prawa. W praktyce, nieumyślne uzyskanie nieuprawnionego dostępu do systemu może nastąpić w zasadzie wyłącznie w sytuacji wejścia do systemu całkowicie niezabezpieczonego przed zdalnym dostępem z cyberprzestrzeni.

Na odrębne potraktowanie zasługuje wreszcie także kwestia dopuszczonych na gruncie Konwencji ograniczeń odpowiedzialności karnej. Zgodnie ze zdaniem drugim art. 2 Konwencji, strony umowy mogą ograniczyć karalność uzyskania nieuprawnionego dostępu do systemu do przypadków, w których dostęp uzyskany został w ramach przełamania zabezpieczeń systemu, czyn popełniono z zamiarem wykradzenia danych bądź innym, określonym przez prawo krajowe zamiarem lub też czyn popełniono „w stosunku do systemu komputerowego połączonego z innym systemem komputerowym" - a więc za pośrednictwem sieci (czyli z wyłączeniem lokalnego włamania do systemu, w którym atakujący siada przed atakowanym komputerem[169]). O ile określanie przez ustawodawców krajowych wymogów popełnienia czynu w określonym zamiarze stanowi głównie element przyjętej polityki karnej, o tyle możliwość ograniczenia karalności dostępu do systemu do przypadków, w których naruszone zostają przez atakującego mechanizmy bezpieczeństwa systemu należy ocenić negatywnie. Po pierwsze - warunek taki oznacza istotne ograniczenie ochrony systemów niezabezpieczonych oraz źle zabezpieczonych. Należy ponownie zwrócić uwagę na brak przepisów, które nakładałyby na prywatne osoby fizyczne obowiązek stosowania jakichkolwiek rozwiązań bezpieczeństwa w swoich systemach. Po drugie zaś - niestosowanie w systemach zabezpieczeń informatycznych, choć wysoce nierozważne, nie może być interpretowane, jako udostępnienie swojego systemu dla całej społeczności cyberprzestrzeni (tak jak niezamknięcie samochodu nie oznacza, że każdy ma prawo nim odjechać!). W praktyce, wprowadzenie karalności jedynie naruszeń polegających na łamaniu zabezpieczeń oznaczałoby wyłączenie ochrony systemów najsłabszych użytkowników, zachęcając cyberprzestępców do polowania na ofiary niepodlegające żadnej ochronie.

Na gruncie prawa europejskiego, karalność uzyskania nieuprawnionego dostępu do systemu informatycznego wprowadzona została na mocy art. 2 Decyzji Ramowej Rady Unii

[169] W ten właśnie sposób zastosowane w Konwencji sformułowanie rozwijane jest w pkt 50 Raportu Wyjaśniającego do Konwencji.

Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[170] oraz następnie zapisana w przepisie art. 3 Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne[171]. Poniżej brzmienia obydwu przepisów, z zachowaniem kolejności chronologicznej:

„Artykuł 2 Nielegalny dostęp do systemów informatycznych

1. Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślny bezprawny dostęp do całości lub części systemu informatycznego jest karalny jako przestępstwo, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.

2. Każde Państwo Członkowskie może zdecydować, że zachowanie, o którym mowa w ust. 1 jest objęte oskarżeniem jedynie w przypadkach, kiedy przestępstwo popełniane jest z naruszeniem zabezpieczenia.” [172]

„Artykuł 3 Niezgodny z prawem dostęp do systemów informatycznych

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne i bezprawne uzyskiwanie dostępu do całości lub jakiejkolwiek części systemu informatycznego, było karalne jako przestępstwo w przypadku, gdy zostało ono popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.” [173]

Pomijając różnice terminologiczne (np. zastosowanie wyrażenia „system informatyczny” zamiast „systemu komputerowego”), przytoczone regulacje Unii Europejskiej zaprojektowane zostały w pełnej spójności z rozwiązaniami Konwencji Rady Europy o cyberprzestępczości. Analogicznie, jak w przypadku dokumentu Rady Europy, uzyskanie nieuprawnionego dostępu do systemu stypizowane zostało w Decyzji oraz zastępującej ją Dyrektywie przy zastosowaniu dwóch, następujących znamion przestępstwa: wystąpienia sytuacji faktycznej, w której sprawca uzyskał dostęp do całości lub części systemu (Konwencja posługiwała się zwrotem „dowolna część”, który nie powoduje jednak różnic interpretacyjnych), oraz kwalifikacji prawnej czynu uzyskania dostępu, jako dostępu „bezprawnego” oraz „umyślnego”.

---

[170] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW.

[171] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

[172] Art. 2 Decyzji Ramowej Rady Unii Europejskiej w sprawie ataków na systemy informatyczne. Przytoczony fragment pochodzi z oficjalnej polskiej wersji językowej dokumentu.

[173] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

O ile samo pojęcie „dostępu do systemu” nie otrzymało definicji legalnej - a co za tym idzie zastosowanie znajdują w tym miejscu wszelkie wcześniejsze uwagi dot. tego określenia, poczynione na gruncie Konwencji, o tyle dokumenty przygotowane przez Unię Europejską wyposażone zostały w definicję wyrażenia „bezprawny”. I tak, zgodnie z lit. d art. 1 Decyzji Ramowej:

> „d) „bezprawne” oznacza dostęp lub ingerencję, na którą właściciel, inny posiadacz prawa do systemu lub jego części nie udzielił zgody lub która nie jest dozwolona na mocy prawa krajowego.” [174].

Stosownie do art. 2 lit d analizowanej Dyrektywy:

> „d) „bezprawnie” oznacza działanie, o którym mowa w niniejszej dyrektywie, w tym dostęp, ingerencje lub przechwycenie, na które właściciel lub inny uprawniony do systemu lub jego części nie udzielił zgody, lub które nie jest dozwolone na mocy prawa krajowego.” [175]

Przytoczone definicja, odpowiadające „informatycznemu” rozumieniu bezprawności dostępu, wskazują dwa źródła „uprawnienia” działań w systemie:

1) zgodę właściciela systemu lub innego posiadacza prawa do systemu lub jego części; oraz,
2) obowiązujący przepis prawa krajowego.

Powyższe rozumienie pojęcia „bezprawności” odpowiada w pełni treści sformułowania „nieuprawnionego dostępu” znanego z Konwencji Budapesztańskiej, ponownie potwierdzając aktualność wcześniejszych uwag, które przedstawione zostały przy okazji postanowień Konwencji o cyberprzestępczości. Należy ocenić, że spójność obu regulacji wpływa pozytywnie na harmonizację prawa w zakresie globalnym - co stanowi oczywiście jeden z filarów skutecznego zwalczania cyberprzestępczości. Brak spójności regulacji prawnych przyjmowanych na różnych kontynentach powoduje jedynie osłabienie systemu prawnego, który w przypadku zwalczania cyberprzestępczości, powinien zachowywać możliwie globalny charakter - odpowiadający charakterowi samej cyberprzestrzeni.

Na marginesie, warto też zaznaczyć, iż opcjonalna na gruncie przepisów Decyzji Rady przesłanka „popełnienia przestępstwa z naruszeniem zabezpieczenia”, stała się przesłanką obligatoryjną dla uznania karalności analogicznego czynu stypizowanego jednak na gruncie

[174] Art. 2 Decyzji Ramowej Rady Unii Europejskiej w sprawie ataków na systemy informatyczne. Przytoczony fragment pochodzi z oficjalnej polskiej wersji językowej dokumentu.

[175] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

postanowień Dyrektywy. Aktualnie zatem – każdy atak, dla dokonania jego prawno karnej kwalifikacji musi być dokonywany „z naruszeniem środków bezpieczeństwa".

W tym miejscu należałoby przejść do prezentacji regulacji krajowych, przyjętych przez ustawodawcę polskiego. Uzyskanie nieuprawnionego dostępu do systemu stypizowane zostało w art. 267 § 2 Kodeksu karnego. Po istotnych zmianach całego art. 267 Kk wprowadzonych w szczególności nowelą z dnia 24 października 2008 r.[176], przepis ten otrzymał krótkie brzmienie:

> „Art. 267. § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.".

Zwrot „tej samej karze" odnosi się do wskazanych w § 1 sankcji w postaci grzywny, kary ograniczenia wolności oraz kary pozbawienia wolności do lat 2.

Wprowadzona do Kodeksu karnego norma art. 267 § 2 stanowi bezpośrednią, niejako automatyczną, implementację regulacji zawartej w komentowanej wyżej Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne. O ile sam przepis nie wymaga w konsekwencji dodatkowego komentarza, który uzupełniałby wcześniejsze uwagi, o tyle zasadne jest dokonanie w tym miejscu oceny samej metody implementacji przepisu.

W pierwszej kolejności należy zatem zwrócić uwagę na brak dokonania przez polskiego ustawodawcę należytej transpozycji terminologicznej, która pozwoliłaby przenieść na grunt prawa polskiego, siatkę pojęciową zastosowaną w przepisach międzynarodowych. Nadając art. 267 § 2 przytoczone brzmienie, prawodawca krajowy zdecydował się wprowadzić nową dla prawa polskiego kategorię „systemu informatycznego"[177]. Prawo polskie operuje w pierwszej kolejności zdefiniowanym pojęciem „systemu teleinformatycznego" (np. ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne[178], wydane do tej ustawy rozporządzenie w sprawie Krajowych Ram Interoperacyjności[179], czy wreszcie ustawa o ochronie informacji niejawnych[180]). Pojęcie „systemu informatycznego" nie posiada zatem na gruncie prawa polskiego swojej definicji[181] - choć jego znaczenie zostało określone legalnie w przepisach implementowanej Decyzji

---

[176] Dz. U. Nr 214, poz. 1344.

[177] A. Lach, op. cit., system LEX - komentarz do art. 267 k.k.

[178] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.)

[179] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 0, poz. 526).

[180] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167, z późn. zm).

[181] Por. M. Siwicki, op. cit., s. 116.

Ramowej (zgodnie z zawartą w Decyzji definicją wyrażenie „system informatyczny oznacza wszelkie urządzenia lub grupę połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez nie w celach ich eksploatacji, użycia, ochrony lub utrzymania"[182].). Zamieszanie terminologiczne komplikuje dodatkowo fakt wprowadzenia do art. 269a Kodeksu karnego wyrażenia „system komputerowy", znanego z kolei z przepisów Konwencji o cyberprzestępczości. Prezentowany automatyzm oraz bezrefleksyjność ustawodawcy krajowego w trakcie implementacji przepisów poszczególnych aktów międzynarodowych do prawa krajowego należy oceniać wyłącznie negatywnie, jako wyraz nieumiejętności rzeczywistego dostosowania prawa polskiego do przyjętych na arenie międzynarodowej standardów.

Po drugie, o ile Decyzja Ramowa zawierała w swoich przepisach definicję „bezprawności" dostępu, o tyle regulacja krajowa została takiej definicji pozbawiona. Ponownie, wymogi zachowania najwyższej precyzji przepisów karnych nie znalazły niestety należytego zastosowania. Jednocześnie, art. 267 Kodeksu karnego posługuje się zwrotem „bez uprawnienia", art. 268, 268a oraz 269a zwrotem „nie będąc do tego uprawnionym", zaś art. 269 pomija zupełnie kwestie bezprawności (czy oznacza to, że nawet uprawnione usuwanie danych informatycznych o szczególnym znaczeniu do obronności podlega karze pozbawienia wolności do lat 8?).

I wreszcie po trzecie - na pełną aprobatę zasługuje podjęcie przez ustawodawcę polskiego decyzji o nieskorzystaniu z przewidzianej w Decyzji Ramowej możliwości ograniczenia odpowiedzialności karnej wyłącznie do przypadków, w których analizowane przestępstwo popełniane jest z naruszeniem zabezpieczenia[183]. Przyjęcie takiego ograniczenia oznaczałoby w praktyce wyłączenie odpowiedzialności za wtargnięcie do systemu niezabezpieczonego lub też źle zabezpieczonego - ominięcie mechanizmów bezpieczeństwa nie jest bowiem tożsame z ich naruszeniem[184]. Należy zaznaczyć, że w pierwotnym brzmieniu art. 267 Kodeksu karnego, komentowany warunek funkcjonował w odniesieniu do uzyskania dostępu do informacji, jednak po spotkaniu się z istotną krytyką doktryny został

[182] Art. 1 lit. a Decyzji Ramowej Rady Unii Europejskiej w sprawie ataków na systemy informatyczne. Przytoczony fragment pochodzi z oficjalnej polskiej wersji językowej dokumentu.

[183] Art. 2 ust. 2 Decyzji Ramowej Rady Unii Europejskiej w sprawie ataków na systemy informatyczne: 2. Każde Państwo Członkowskie może zdecydować, że zachowanie, o którym mowa w ust. 1 jest objęte oskarżeniem jedynie w przypadkach, kiedy przestępstwo popełniane jest z naruszeniem zabezpieczenia.". Przytoczony fragment pochodzi z oficjalnej polskiej wersji językowej dokumentu.

[184] W. Wróbel, op. cit., system LEX - komentarz do art. 267 k.k.

zniesiony przywołaną wcześniej nowelą z 2008 r.

§4. Cyberprzestępstwa związane z dokonywaniem nieuprawnionych czynności wewnątrz systemu.

Trzecia spośród wyróżnionych w zaproponowanym ujęciu kategorii cyberprzestępstw, obejmuje czyny, które dokonywane są „wewnątrz" atakowanego systemu, a zatem już poza obszarem samej transmisji danych, a także po przekroczeniu granicy systemu ofiary. Tak określona kategoria cyberprzestępczości odpowiada w konsekwencji czynom popełnianym na ostatnim etapie ruchu danych w cyberprzestrzeni, który to ruch można scharakteryzować uproszczonym schematem: transmisja danych przez sieci - dopuszczenie danych do wnętrza systemu - przetwarzanie danych wewnątrz systemu (działania w systemie). Podobnie, jak w przypadku uzyskiwania nieuprawnionego dostępu do systemu, transmisja danych stanowi niezbędne medium dla nielegalnego pozyskania informacji, jednak nie wyznacza samego obszaru popełnienia przestępstwa. W ramach cyberprzestępstw związanych z dokonywaniem nieuprawnionych czynności wewnątrz systemu, na gruncie obowiązujących w kraju przepisów karnych wyróżnić można dwa następujące rodzaje cyberprzestępstw:

1) uzyskanie nieuprawnionego dostępu do informacji przetwarzanej w systemie; oraz,
2) wprowadzanie nieuprawnionych zmian w systemie, w tym:
   a) wprowadzanie nieuprawnionych zmian powodujących zakłócenia pracy systemu, jako całości, oraz
   b) wprowadzanie nieuprawnionych zmian, które nie wywołują takich zakłóceń.

Od strony technicznej, cyberprzestępstwa związane z dokonywaniem nieuprawnionych czynności wewnątrz systemu, polegają na całościowym lub częściowym przejęciu kontroli nad atakowanym systemem. Celem takiego działania jest uzyskanie przez atakującego możliwości wydawania atakowanemu systemowi określonych poleceń lub też wymuszenie na tym systemie określonego zachowania. Wydawane przez atakującego polecenia mogą powodować zarówno określone przetworzenia danych zapisanych w systemie (usunięcie, uszkodzenie, czy też przesłanie danych do innego systemu), jak również wpływać na samą pracę systemu (np. wyłączać jego zabezpieczenia sieciowe). Z punktu widzenia skali skutków wywołanych nieuprawnionymi działaniami, wprowadzone w systemie zmiany mogą pozostawać zarówno nieistotne dla pracy całego systemu, obejmując np. jedynie wybrane pliki dokumentów, jak również powodować dysfunkcje systemu, aż do pełnego przerwania

jego działania.

Poruszone wyżej przejęcie kontroli nad systemem może mieć charakter zarówno *bezpośredni*, jak i *pośredni* (pojęcia te wprowadzam na potrzeby uwidocznienia różnic dzielących określone metody ataku). Przejęciem bezpośrednim nazywam przejęcie będące bezpośrednim następstwem uprzedniego ataku ukierunkowanego, zmierzającego do uzyskania nieuprawnionego dostępu do ściśle określonego systemu (tzw. atak ukierunkowany) - przejęcie to polega w konsekwencji na uzyskaniu dostępu do wybranego systemu oraz wykorzystaniu przez atakującego zdobytej w ten sposób możliwości wydawania „złamanemu" systemowi dowolnych poleceń w czasie rzeczywistym (np. wydanie polecenia wyświetlenia zawartości dysków twardych, polecenia przesłania określonych zasobów, czy też polecenia skasowania wybranych plików). Za przejęcie pośrednie uważam natomiast przejęcie wykonywane dwuetapowo, z zastosowaniem oprogramowania złośliwego, którego działanie nie jest nacelowane na określony system (tzw. atak nieukierunkowany) - np. przejęcie cudzej maszyny poprzez jej zainfekowanie wirusem komputerowym. W takim przypadku moment faktycznego uzyskania nieuprawnionego dostępu do systemu staje się niezwykle trudny do uchwycenia od strony formalnej, bowiem konstytuujące ten moment wprowadzenie oprogramowania złośliwego, tu wirusa, najczęściej dokonywane jest samodzielnie - choć oczywiście w sposób nieświadomy, przez uprawnionego użytkownika systemu (np. w trakcie pobierania zarażonych dokumentów, czy też odtwarzania *on-line* filmów bądź muzyki). Wprowadzone oprogramowanie złośliwe może następnie realizować w zasadzie dowolne, nieuprawnione działania - od ujawniania materiałów przetwarzanych na komputerze, przez modyfikowanie jego zasobów oraz ustawień, aż po sformatowanie dysków twardych. Warto podkreślić, że już samo wprowadzenie do wnętrza atakowanego systemu oprogramowania złośliwego konstytuuje wprowadzenie nieuprawnionej zmiany w systemie - dalsze działania takiego oprogramowania, powodują kolejne, również nieuprawnione zmiany. Metoda przejęcia pośredniego stosowana jest na szeroką skalę także w ramach tworzenia tzw. *botnetów*, czyli sieci „zdalnie sterowanych" komputerów, które mogą być następnie wykorzystywane w celach przestępnych (o *botnetach* pisano szerzej w poprzednich częściach pracy). Niezależnie od zastosowanej metody ataku, cyberprzestępstwa związane z wykonywaniem nieuprawnionych czynności w systemie, polegają nie tyle na uzyskaniu dostępu do atakowanego systemu (choć działanie to stanowi niezbędny etap przejęcia kontroli), co wydawaniu mu, w sposób nieuprawniony, poleceń określonego zachowania.

Metody uzyskania nieuprawnionego dostępu do systemu były przedmiotem analiz w poprzedniej części rozdziału.

1. Uzyskanie nieuprawnionego dostępu do informacji przetwarzanej w systemie

Wprowadzona przez ustawodawcę polskiego odrębna karalność czynu polegającego na uzyskaniu nieuprawnionego dostępu do informacji przetwarzanej w systemie, stanowi rozwiązanie prawne, które nie zostało przewidziane wprost ani w przepisach Konwencji Rady Europy o cyberprzestępczości, ani Decyzji Ramowej Rady Unii Europejskiej w sprawie ataków na systemy informatyczne, stanowiących punkt odniesienia prawnego dla regulacji krajowych. Obydwa wskazane akty prawa międzynarodowego typizują bowiem przede wszystkim uzyskanie nieuprawnionego dostępu do systemu, którego karalność nie jest uzależniana od tego, czy ów dostęp do systemu nastąpił w połączeniu z (choćby hipotetyczną) możliwością uzyskania dostępu do jakichkolwiek przetwarzanych w tym systemie informacji. Niemniej jednak, należy zaznaczyć, że Konwencja o cyberprzestępczości w swoim art. 3 (zatytułowanym „Bezprawne przechwytywanie") wprowadziła m. in. penalizację czynu polegającego na przechwytywaniu transmisji dokonywanej wewnątrz systemu - a zatem pomiędzy jego poszczególnymi komponentami (np. dyskiem twardym, procesorem oraz pamięcią operacyjną). Czyn taki nie jest *de facto* dokonywany w obszarze transmisji danych w cyberprzestrzeni, zaś wypełnia cechy nieuprawnionego uzyskiwania dostępu do treści przetwarzanych przez atakowany system wyłącznie lokalnie - to jest w obrębie tego systemu. Karalność tzw. podsłuchu komputerowego (to jest przestępstwa popełnianego w obszarze transmisji danych) prezentowana była szeroko w części 1 rozdziału.

Przytaczany już wcześniej art. 3 Konwencji stanowi, że:

> „Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego, popełnionego umyślnie czynu polegającego na bezprawnym przechwytywaniu danych komputerowych przekazywanych do, z lub wewnątrz systemu komputerowego w ramach transmisji o nie-publicznym charakterze, dokonywanym przy użyciu środków technicznych, w tym przechwytywanie ulotu elektromagnetycznego systemu komputerowego, zawierającego takie dane komputerowe. Strona może wprowadzić dodatkowe wymogi popełnienia przestępstwa z nieuczciwym zamiarem lub w stosunku do systemu komputerowego, który połączony jest z innym systemem komputerowym."[185].

[185] Art. 3 Konwencji o cyberprzestępczości. W oryginale: „*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of*

Skupiając się w tym miejscu jedynie na kwestii karalności uzyskania nieuprawnionego dostępu do informacji przetwarzanej w systemie, należy zauważyć, że na gruncie Konwencji, jako przestępne uznane zostało działanie:

- polegające na bezprawnym przechwytywaniu danych komputerowych (nie zaś informacji) przekazywanych wewnątrz systemu komputerowego w ramach transmisji o nie-publicznym charakterze, oraz,
- dokonywane przy użyciu środków technicznych (środkiem takim może być sam komputer sprawcy ataku).

Jak stanowi pkt 55 Raportu Wyjaśniającego do Konwencji, przekazywanie danych wewnątrz pojedynczego systemu komputerowego to ruch danych pomiędzy poszczególnymi komponentami systemu (przykładowo „procesorem, a monitorem lub drukarką")[186]. Nie-publiczny charakter transmisji oznacza zaś w skrócie, że przekazywanie danych nie miało mieć, w zamierzeniu właściciela systemu, charakteru otwartego, kierującego dane do nieoznaczonego kręgu adresatów (*vide* wcześniejsze uwagi poczynione w części 1 rozdziału). Co istotne, przepis nie penalizuje uzyskiwania dostępu do informacji, zaś uzyskiwanie dostępu do danych. Należy zaznaczyć, że nie każde „dane" składają się na informację (np. dane zaszyfrowane), a zatem pojęcia te posiadają różny zakres semantyczny. O ile każda informacja zapisana na komputerze wyrażona jest w postaci danych, o tyle nie każde dane muszą składać się na informację. W pewnym sensie można powiedzieć, że pojęcie „danych komputerowych" stanowi kategorię obiektywną, podczas gdy kwalifikacja „informacji" zawsze wymaga dokonania swoistej oceny, czy pozyskane przez sprawcę cyberprzestępstwa dane już kształtują informację. Ponownie, kwestie te były przedmiotem szerszych analiz w części 1 rozdziału.

Na tle zastosowanego w przepisie sformułowania „przechwytywanie danych przekazywanych wewnątrz systemu", zasadne staje się postawienie pytania o rzeczywisty zakres opisywanego w ten sposób czynu. Działania polegające wyłącznie na powodowaniu przekazywania danych wewnątrz systemu (np. wydane zdalnie polecenie otwarcia na komputerze pliku zawierającego oprogramowanie złośliwe) z pewnością nie wypełniają znamienia „przechwytywania", wymykając się w efekcie przyjętej redakcji przepisu. Zgodnie z art. 3 Konwencji, penalizowane są w efekcie wyłącznie te działania, które powodują

---

computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.". Tłumaczenie własne.

[186] W oryginale, odnośne zdanie stanowi, że: „*The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example)* [...]".

pozyskanie danych. Bez znaczenia pozostaje w tym miejscu fakt, czy stanowiące przedmiot przestępstwa dane zostały otwarte przez atakującego, czy ich przetwarzanie (umożliwiające podsłuch) zostało zainicjowane przez uprawnionego użytkownika systemu.

Przechodząc do analizy regulacji krajowej, czyn uzyskania nieuprawnionego dostępu do informacji został stypizowany w art. 267 § 1 Kodeksu karnego. Przepis ten posiada aktualnie następujące brzmienie:

> „Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.”.

Zgodnie z przyjętą redakcją przepisu, na gruncie polskiego prawa zabronione zostało nieuprawnione uzyskanie dostępu do informacji, noszące następujące znamiona:

- informacja objęta przestępstwem musi mieć charakter „informacji nieprzeznaczonej” dla sprawcy,
- uzyskanie dostępu musi nastąpić w ramach otwarcia zamkniętego pisma, podłączenia się do sieci telekomunikacyjnej lub w drodze przełamania albo ominięcia szczególnego zabezpieczenia danej informacji - w tym zabezpieczenia informatycznego[187].

Powyższa konstrukcja przestępstwa nasuwa szereg istotnych uwag pojawiających się w kontekście specyfiki przestępczości cyberprzestrzeni.

Po pierwsze, odniesienie całego czynu do „informacji”, oznacza karalność wyłącznie takich działań, których przedmiotem stało się uzyskanie dostępu do informacji, nie zaś wyłącznie danych - *vide* wcześniejsze uwagi. W szczególności, oznacza to, że dostęp do danych nie składających się na informacje (np. dane zaszyfrowane, dane fragmentaryczne niepoddające się odczytowi, czy wreszcie elementy samego oprogramowania nie zawierające informacji) wymyka się spod przyjętej regulacji karnej. Jednocześnie, dla zaistnienia analizowanego przestępstwa bez znaczenia pozostaje fakt, czy informacja, do której sprawca czynu uzyskał dostęp jest informacją przez niego poszukiwaną, czy też w ogóle interesującą[188].

Po drugie, zastosowanie przesłanki „uzyskania dostępu” nie wprowadza wymogu, aby

---

[187] W. Wróbel, op. cit., system LEX - komentarz do art. 267 k.k.
[188] M. Kalitowski, op. cit., s. 1144.

sprawca przestępstwa rzeczywiście zapoznał się z jakąkolwiek informacją. Poprzez uzyskanie dostępu, należy bowiem rozumieć taki stan, w którym sprawca *czynu* uzyskał faktyczną, obiektywną możliwość przeczytania informacji zapisanej na komputerze[189]. Jednocześnie, nie można zapominać, że nie każde uzyskanie dostępu do systemu oznacza równoległe uzyskanie możliwości zapoznawania się z zasobami przetwarzanymi w tym systemie - np. możliwe jest częściowe przełamanie zabezpieczeń systemu zezwalające na przeglądanie struktury katalogów oraz plików na dysku, jednak nie samo otwieranie plików. Czyn tak będzie mógł zostać zakwalifikowany, jako podlegający sankcji dostęp do informacji, wyłącznie w przypadku, o ile same nazwy katalogów oraz plików zostaną uznana za „informacje". Bez względu na wynik takiej kwalifikacji, opisany w poprzednim zdaniu czyn wypełni natomiast przesłanki nieuprawnionego dostępu do systemu (stypizowanego w art. 267 § 2 Kodeksu karnego).

Po trzecie, zastosowana w przepisie cecha „przeznaczenia" informacji dla określonej osoby, nie posiada jednoznacznej treści semantycznej. W szczególności, za nieuzasadnione uważam utożsamianie treści zastosowanego pojęcia z określeniem kręgu adresatów danej informacji[190]. Pogląd taki nie tylko nie znajduje poparcia w samym brzmieniu przepisu (brak w jego redakcji określenia „adresat", które mogło przecież być wprowadzone przez ustawodawcę), ale także pomija kwestie istotne z punktu widzenia specyfiki cyberprzestępczości. Wprowadzając bowiem komentowany przepis do obszaru cyberprzestrzeni, należy zwrócić uwagę na szczególne wątpliwości związane z określaniem kręgu użytkowników, dla których dana informacja została przeznaczona:

- czy fakt bycia adresatem informacji oznacza automatyczne udzielenie użytkownikowi dostępu do tej informacji w dowolnym systemie?,
- czy informacje już posiadane przez użytkownika - w tym przez niego wytworzone, mogą być kwalifikowane, jako informacje dla niego nieprzeznaczone z uwagi na samo umiejscowienie systemu, w którym są przetwarzane? (np. kazus włamania się pracownika do własnych zasobów umieszczonych na firmowym serwerze celem ich zdalnego wykradzenia oraz sprzedaży konkurencji), oraz,
- czy nieuprawnione uzyskanie dostępu do informacji, do której posiada się także legalny dostęp (np. włamanie się do zasobów systemu, do których posiada się hasło legalnego wstępu), stanowi bezprawne uzyskanie dostępu do informacji nieprzeznaczonej dla sprawcy tak opisanego czynu?

---

[189] Por. M. Siwicki, op. cit., s. 112 i nast.
[190] *Ibidem*, s. 1143 i 1144.

Powyższe pytania pozwalają zarysować specyficzne trudności związane z identyfikacją oraz przydziałem uprawnień użytkowników do korzystania z zasobów, w tym informacji, przetwarzanych w systemach. W obszarze cyberprzestrzeni bowiem, przeznaczenie informacji dla danego użytkownika powinno być oceniane w szczególności w kontekście uprawnień, jakie użytkownik ten posiada w danym systemie. Wyłączenie uprawnień określonej osoby do działania w systemie oznaczać musi w konsekwencji, że żadna z informacji przetwarzanych w tym systemie nie jest przeznaczona dla takiej osoby - nawet jeśli jest ona adresatem przedmiotowej informacji (np. adresat wiadomości pocztowej zapisanej w skrzynce *e-mail* nadawcy). Jednocześnie, brak technicznego ograniczenia dostępu użytkownika do wybranych zasobów systemu, nie oznacza jego dopuszczenia do wszelkich materiałów przetwarzanych w tym systemie - kwestię uprawnień użytkownika do dostępu do informacji należy bowiem odróżnić od przyznanych mu w systemie możliwości lub też uprawnień technicznych (np. administrator systemu pocztowego może zostać dopuszczony do zmiany zapomnianych haseł, jednak nie uprawnia go to do „wyrabiania" sobie dodatkowych haseł i przeglądania cudzej poczty).

W kontekście przywołanych wątpliwości, należy zauważyć, że analizowana regulacja karna nie pozwala na przeprowadzanie kwalifikacji czynów dokonywanych w systemach wprawdzie bezprawnie, jednak w odniesieniu do informacji, które nie są „nieprzeznaczone" dla sprawcy - jak choćby przywołany wcześniej przykład uzyskania nieuprawnionego dostępu do własnej poczty obsługiwanej jednak przez serwer pracodawcy, celem wykradzenia zawartych na niej materiałów. Czyny takie nie spełniają bowiem przesłanek wymienionych kumulatywnie na gruncie art. 267 § 1 Kodeksu karnego. Swoistą lukę przyjętej regulacji wypełnia natomiast art. 267 § 2 Kodeksu karnego - sankcjonujący samo bezprawne uzyskanie dostępu do systemu[191], prezentowany szeroko w poprzedniej części rozdziału.

Po czwarte - wracając do analizy przestępstwa opisanego w art. 267 § 1 Kodeksu karnego, stypizowane w tym przepisie uzyskanie dostępu do informacji musi nastąpić w ramach otwarcia zamkniętego pisma, podłączenia się do sieci telekomunikacyjnej lub też w drodze przełamania albo ominięcia szczególnego zabezpieczenia informacji, w tym zabezpieczenia informatycznego. Należy stwierdzić, że w odniesieniu do cyberprzestępstwa uzyskania bezprawnego dostępu do informacji, zastosowanie znajduje każda z tych przesłanek:

[191] W. Wróbel, op. cit., system LEX - komentarz do art. 267 k.k.

- w związku z postępującą informatyzacją życia, pod pojęciem „pisma" nie należy rozumieć dziś już tylko dokumentów w postaci papierowej, ale także dokumenty elektroniczne. Interpretacja ta znajduje pełne poparcie m. in. w przepisach Kodeksu postępowania administracyjnego[192], np. art. 39^1 oraz 46 – przewidujących doręczanie pism za pomocą środków komunikacji drogą elektroniczną. Konieczne w tym miejscu staje się jednak poprawne odniesienie do pisma elektronicznego zwrotu „otwarcie zamkniętego pisma". W stosunku do pism konwencjonalnych, zwrot ten rozumiany jest przykładowo, jako „rozerwanie, przecięcie, odklejenie koperty, złamanie pieczęci, odplombowanie"[193], czyli zbiór prostych czynności technicznych mających na celu uzyskanie dostępu do treści pisma ukrytej przed wzrokiem. Jednocześnie, czynności te powodują wyraźne uszkodzenia zabezpieczenia pisma, które wskazuje jego właściwego adresata. Ponieważ pisma elektroniczne nie wymagają kopert, zaś przekazywane są za pośrednictwem sieci w postaci impulsów elektrycznych (reprezentujących z kolei bity informacji) - w ocenie autora niniejszej pracy, należy przyjąć, że otwarciem pisma elektronicznego jest samo pobranie jego treści przez sieć (doręczenia pism administracyjnych dokonywane są przy zastosowaniu specjalnego mechanizmu weryfikacji pobrania pisma) lub też otwarcie otrzymanej wiadomości pocztowej - wymagające w obydwu przypadkach aktywnego udziału osoby uzyskującej dostęp do informacji. O ile zatem z okoliczności sprawy wynika, że sprawca czynu świadomie otwierał pismo nieprzeznaczone dla niego - rolę koperty spełniać może przykładowo nagłówek wiadomości *e-mail*, czynności techniczne mające na celu wyświetlenie treści pisma należy uznać, że spełniające znamię „otwarcia zamkniętego pisma". Otwarciem takim nie jest natomiast otworzenie pliku, który nie posiada należytego opisu lub został przesłany za pustą wiadomością,
- uzyskanie informacji poprzez podłączenie się do sieci telekomunikacyjnej prezentowane było szerzej w części 1 rozdziału. W tym miejscu należy jedynie zauważyć, że wszelkie działania dokonywane za pośrednictwem sieci wypełniają to znamię, niezależnie od tego, czy samo podłączenie do sieci miało charakter bezprawny, czy też było w pełni legalne (przesłanka wymaga wyłącznie działania związanego z połączeniem z siecią). W konsekwencji, każde działanie dokonywane

[192] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, Dz. U. Nr 30, poz. 168, z późn. zm.
[193] M. Kalitowski, op. cit., s. 1144.

w cyberprzestrzeni dokonywane jest jednocześnie poprzez podłączenie się do sieci telekomunikacyjnej,

- przełamanie bądź też ominięcie zabezpieczenia informacji wiążę się z uzyskaniem dostępu do informacji, której treść została zabezpieczona w szczególny sposób. Typowymi zabezpieczeniami informatycznymi są narzędzia ograniczające dostęp do określonych zasobów systemu (np. plików umieszczonych w danym katalogu) chronionych hasłem oraz narzędzia kryptograficzne, przekształcające czytelną wiadomość w tzw. szyfrogram. Należy zaznaczyć, że współcześnie same systemy operacyjne wyposażone są w rozliczne zabezpieczenia dostępu, chroniące przetwarzane dane zarówno przed atakami sieciowymi, jak również lokalnymi (gdy atakujący siada bezpośrednio przed atakowanym komputerem). Zabezpieczenia takie również winny być traktowane, jako „szczególne zabezpieczenia informacji", o których stanowi przepis.

Ostatecznie, znamię „braku uprawnienia" uzyskania dostępu do informacji musi być oceniane w odniesieniu do praw wyłącznych właściciela systemu, o czym pisano w poprzedniej części rozdziału. Uprawnienie do wykonywania wszelkich czynności w systemie przysługuje w konsekwencji wyłącznie jego właścicielowi, którzy poprzez nadawanie praw innym użytkownikom lub też instalację wybranych programów (a co za tym idzie przyjmowanie związanych z tym oprogramowaniem warunków umów licencyjnych) oraz odpowiednią konfigurację systemu, może dysponować swoimi prawami, wyznaczając sfery, nad którymi traci wyłączną kontrolę w systemie. Uprawnienie do działania w systemie może także wynikać z mocy powszechnie obowiązującego przepisu prawnego.

2. Wprowadzanie nieuprawnionych zmian w systemie

Przestępstwo wprowadzania nieuprawnionych zmian w systemie polega na dokonywaniu wewnątrz zaatakowanego systemu jakichkolwiek modyfikacji, które nie zostały należycie autoryzowane przez właściciela lub uprawnionego gestora systemu (np. jego administratora). Z uwagi na zasady rządzące strukturą oraz funkcjonowaniem cyberprzestrzeni, przedmiotem zmian są zawsze dane komputerowe, które odzwierciedlają jednak szereg zróżnicowanych zasobów - dane mogą wyrażać zarówno informacje zapisane w formie dokumentów tekstowych, składać się na pliki muzyczne lub filmowe, budować programy komputerowe - w tym także systemy operacyjne, jak również opisywać określone ustawienia systemowe (np. wskazywać, które porty sieciowe są otwarte, a które zamknięte na

ruch przychodzący z sieci). W efekcie, stosując kryterium rozległości skutków wywołanych w systemie wprowadzeniem nieuprawnionych zmian, tę kategorię cyberprzestępstw można podzielić na cyberprzestępstwa zakłócające pracę systemu oraz cyberprzestępstwa niewywołujące takiego efektu.

Wprowadzanie nieuprawnionych zmian powodujących zakłócenia pracy systemu

Poprawne funkcjonowanie systemu oparte jest w największej mierze na niezakłóconym działaniu oprogramowania, które zostało zainstalowane wewnątrz systemu. W szczególności, twierdzenie to dotyczy systemów operacyjnych, stanowiących centralne oprogramowanie, zawiadujące pracą wszystkich pozostałych aplikacji. Wprowadzenie modyfikacji w tych zasobach systemu, od których uzależnione jest realizowanie funkcji systemu, może w konsekwencji doprowadzić do częściowego zaburzenia działania systemu (np. wyłączenia określonych usług lub programów), a nawet całkowitego wyłączenia lub zawieszenia systemu. Jako przykłady działań wywołujących takie efekty można wskazać usunięcie bądź uszkodzenie plików istotnych programów komputerowych, modyfikację ustawień systemu powodującą zaburzenia w jego pracy (np. odcięcie od sieci), jak również wydawanie *przełamanemu* systemowi poleceń wpływających negatywnie na realizację powierzonych mu do realizacji zadań (jak choćby proste polecenie zresetowania maszyny, krótkotrwale wyłączające jej dostępność dla uprawnionych użytkowników)[194].

Zgodnie z art. 5 Konwencji Rady Europy o cyberprzestępczości:

> „Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego, popełnionego umyślnie czynu polegającego na istotnym, bezprawnym zakłócaniu funkcjonowania systemu komputerowego poprzez wprowadzanie, transmisję, niszczenie, usuwanie, uszkadzanie, modyfikowanie lub utrudnianie dostępu do danych komputerowych”[195].

Co było przedmiotem wcześniejszych rozważań, przytoczony przepis obejmuje swoim zakresem przedmiotowym nie tylko działania dokonywane wewnątrz atakowanego systemu, ale także zakłócenia pracy systemu powodowane „zalewaniem” systemów nadmierną transmisją danych (atak typu *denial-of-service*). Zagadnienia karalności cyberprzestępstw

[194] Por. M. Siwicki, op. cit., s. 135.
[195] W oryginale: „*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*”. Tłumaczenie własne.

popełnianych w obszarze transmisji danych stanowią przedmiot rozważań zawartych w części 1 rozdziału.

Analizując treść art. 5 Konwencji pod kątem penalizacji wywoływania zakłóceń w pracy systemu poprzez dokonywanie nieuprawnionych działań wewnątrz systemu, należy zauważyć, że w przepisie tym stypizowano czyn istotnego zakłócenia funkcjonowania systemu komputerowego, które dokonane zostało poprzez:

- wprowadzenie,
- transmisję (która zgodnie z Raportem Wyjaśniającym do Konwencji obejmuje także przesyłanie danych pomiędzy poszczególnymi komponentami systemu, np. procesorem, a pamięcią - a zatem wewnątrz systemu[196]),
- niszczenie,
- usuwanie,
- uszkadzanie, lub też
- modyfikowanie danych komputerowych[197].

Jako osobne znamię wykonawcze, komentowany przepis wyróżnił także utrudnianie dostępu do danych komputerowych, które w kontekście wprowadzania nieuprawnionych zmian w systemie, należy traktować, jako ewentualne następstwo wykonania, którejś z wymienionych wyżej czynności. Innymi słowy, dla utrudnienia dostępu do jakichkolwiek danych, konieczne w przypadku analizowanych przestępstw jest dokonanie określonych modyfikacji danych - bądź samych danych, do których zamierza się utrudnić dostęp (np. uszkodzenie pliku bazodanowego), bądź też tych danych, które wykorzystywane są dla zapewniania owego dostępu do danych stanowiących przedmiot utrudnienia dostępu (np. uszkodzenie pliku programu komputerowego służącego do otwierania dokumentów tekstowych).

Wyrażenie „wprowadzanie" danych, należy rozumieć szeroko, jako zarówno wgrywanie do systemu danych przygotowanych wcześniej (np. odpowiednio spreparowane oprogramowanie złośliwe), jak również wytwarzanie nowych danych w atakowanym systemie (np. utworzenie krótkiego polecenia). Co zostało podkreślone już wyżej, znamienia „transmisji" danych nie należy odnosić wyłącznie do przestępstw popełnianych w obszarze

[196] Pkt 55 Raportu Wyjaśniającego do Konwencji. *Explanatory Report*, pełen tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[197] W oficjalnym przekładzie Konwencji wymienione w przepisie czynności sprawcze zostały przetłumaczone, jako: wprowadzanie, transmisja, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych.

transmisji danych w cyberprzestrzeni - to jest w ramach transmisji dokonywanej poprzez sieci. W rozumieniu tego pojęcia przedstawionym w Raporcie Wyjaśniającym do Konwencji, transmisja danych obejmuje bowiem także przesyłanie danych pomiędzy poszczególnymi komponentami systemu, a więc w jego wnętrzu. Pojęcia niszczenia, usuwania, uszkadzania oraz modyfikowania odnoszą się z kolei do dokonywania zmian w stosunku do już istniejących danych komputerowych. Istotą usuwania danych, jest oczywiście uczynienie ich całkowicie niedostępnymi, podczas gdy niszczenie lub uszkadzanie danych ma wyłączyć dalszą możliwość poprawnego przetwarzania danych. Jednocześnie, modyfikacja danych - która *de facto* obejmuje także niszczenie oraz uszkadzanie danych, nie oznacza uczynienia danych niezdatnymi do wykorzystania, a wręcz przeciwnie, odnosi się do przypadków, w których przerobione (lub też podrobione) dane traktowane są przez system, jako wiarygodne, wprowadzone do systemu w sposób legalny. Wymieniony katalog działań na danych komputerowych należy uznać za kompletny, obejmujący wszystkie etapy przetwarzania danych w ujęciu technicznym (to jest od zapisu danych, przez ich modyfikację oraz przenoszenie, aż do usunięcia). Co istotne, żadna z czynności nie została odniesiona do danych przetwarzanych w określony sposób, a zatem uregulowane w art. 5 Konwencji przestępstwo może zostać popełnione zarówno względem danych zapisanych na trwałych nośnikach pamięci (np. dysku twardym, czy pamięci typu *flash*), ale również danych przetwarzanych w systemie (np. przetwarzanych przez procesor lub przekazywanych do pamięci operacyjnej systemu).

Co wynika wprost z redakcji art. 5 Konwencji, obowiązkiem penalizacji zakłócenia pracy systemu, objęto wyłącznie przypadki takiego zakłócenia, które może być kwantyfikowane, jako „istotne". O ile sama Konwencja nie zdefiniowała tego pojęcia, o tyle jego znaczenie zostało przybliżone częściowo w Raporcie Wyjaśniającym do Konwencji. W pierwszej kolejności, Raport wskazał na uprawnienie państw-stron Konwencji do samodzielnego określenia katalogu zakłóceń pracy systemu, które winny być uznawane za „istotne". Po drugie zaś, Raport wskazał przykładowo, że istotnymi zakłóceniami pracy systemu są w szczególności zakłócenia mający istotny wpływ na możliwość korzystania z tego systemu oraz zakłócenia ograniczające możliwości komunikacyjne systemu - w tym zakłócenia wywoływane działaniem złośliwego oprogramowania, np. wirusów komputerowych, które blokuje lub wydatnie spowalnia pracę zaatakowanego systemu, czy też blokuje możliwości komunikacji dokonywanej za pośrednictwem systemu, np. poprzez

przeładowanie skrzynki poczty elektronicznej nadmierną ilością niechcianych wiadomości[198]. *A contrario,* jako „nie-istotne", a zatem wyłączone spod penalizacji karnej, winny być te przypadki zakłócenia pracy systemu, które nie wpływają na jego podstawową funkcjonalność oraz realizację głównych zadań. Zarówno zakres podstawowej funkcjonalności, jak i określenie, które spośród zadań systemu należy oceniać, jako główne, musi być dokonywane w odniesieniu do konkretnych przypadków. Przykładowo, system, którego zadaniem jest dokonywanie obliczeń na pieniądzach, potencjalnie może realizować swoje zadanie w sposób niezakłócony nawet w przypadku pozbawienia go wybranych funkcjonalności sieciowych. Z kolei system, którego zadaniem jest wykonywanie operacji poprzez sieci, może zostać wyraźnie spowolniony nawet najmniejszym zakłóceniem jego zdolności komunikacyjnych. Wprowadzoną relatywizację odpowiedzialności karnej, ograniczającą karalność zakłócenia pracy systemu wyłącznie do niezdefiniowanych przypadków „istotnego zakłócenia", należy oceniać, jako wyraz niezdolności państw do wypracowania jednolitych standardów prawnych w zakresie ochrony cyberprzestrzeni.

Zgodnie z przyjętym brzmieniem art. 5 Konwencji, aktualizacja karalności zakłócenia pracy systemu wymaga, aby owo zakłócenie było kwantyfikowane, jako istotne, wyłączając tym samym penalizację przypadków mniejszej wagi.

Pośród przepisów unijnych, przestępstwo wprowadzenia nieuprawnionych zmian wywołujących zakłócenie pracy systemu stypizowane zostało w art. 3 Decyzji Ramowej Rady Nr 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[199] oraz następnie usankcjonowane regulacją art. 6 Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne[200]. Pierwszy z przywołanych przepisów, to jest pochodzący z Decyzji Ramowej - zatytułowany „Nielegalna ingerencja w system", otrzymał następujące brzmienie:

> „Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślne poważne naruszenie lub przerwanie funkcjonowania systemu informatycznego poprzez wprowadzanie, przekazywanie, uszkadzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych jest karalne jako przestępstwo, kiedy dokonane jest bezprawnie, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.".

[198] Pkt 67 Raportu Wyjaśniającego.
[199] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW.
[200] Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

Przepis Dyrektywy zapisano natomiast w postaci:

> „Artykuł 4 Niezgodna z prawem ingerencja w systemy
>
> Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne i bezprawne poważne utrudnienie lub zakłócenie funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych lub czynienie ich niedostępnymi, było karalne jako przestępstwo, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi."

Pomimo drobnych różnic redakcyjnych, przepisy Decyzji Ramowej oraz Dyrektywy stanowią w istocie odzwierciedlenie wskazanej wyżej regulacji Konwencji o cyberprzestępczości. Poczynione wobec niego uwagi znajdują swoje zastosowanie także i w tym przypadku.

Analogicznie, jak w przypadku przestępstwa opisanego w art. 5 Konwencji, przywołana regulacja Decyzji Ramowej wprowadziła penalizację czynu bezprawnego wpłynięcia na funkcjonowanie systemu, w tym wypadku opisanego jednak z zastosowaniem dwóch alternatywnych - choć w pełni kompatybilnych znamion, to jest przy użyciu zwrotu „poważne naruszenie lub przerwanie funkcjonowania systemu". Postanowienie Dyrektywy wprowadziło w to miejsce wyrażenie „poważne utrudnienie lub zakłócenie funkcjonowania systemu informatycznego", które czytane w całości należy jednak traktować jako równoważne treściowo. W kontekście brzmienia postanowień Decyzji, należy zaznaczyć, że różnica w określeniu zastosowanego w analizowanym przepisie znamienia „naruszenia" oraz znamienia „zakłócenia" stosowanego na gruncie Konwencji, w istocie zachowuje wymiar wyłącznie redakcyjny. Co więcej, w wersjach anglojęzycznych obydwu dokumentów znamiona te nazywane są wręcz jednym określeniem „*hindering*" (tłumaczenie „zakłócanie" przyjęto za obowiązującymi przepisami Kodeksu karnego). Jednocześnie, druga przesłanka z przepisu Decyzji - „przerwania funkcjonowania systemu", stanowi określenie takiego zakłócenia, które całkowicie wyłącza pracę zaatakowanego systemu. Bez wątpienia każdy przypadek przerwania funkcjonowania systemu wypełnia tym bardziej znamiona naruszenia, czy też zakłócenia pracy systemu, co przesądza o zgodności zakresów przedmiotowych regulacji Decyzji Ramowej oraz Konwencji. Odnosząc przedstawiane uwagi na grunt postanowień Dyrektywy – ta również w wersji anglojęzycznej posługuje się poruszanym pojęciem „*hindering*" przetłumaczonym jednak w oficjalnej polskiej wersji dokumentu, jako „utrudnianie". Należy także uznawać, że zastosowany w Dyrektywie zwrot „utrudnienie lub zakłócenie funkcjonowania systemu" buduje przesłankę łagodniejszą, łatwiejszą do spełnienia, niż analizowany wyżej przepis Decyzji Ramowej – bowiem w żadnym zakresie

nie wymaga zupełnego „sparaliżowania" pracy systemu. Wystarczające w tym miejscu staje się w istocie samo zaburzenie poprawnej, typowej pracy systemu.

Odnośnie wyliczonych w komentowanych przepisach sposobów wywołania zakłócenia pracy systemu, wprowadzone do regulacji katalogi działań również ocenić należy, jako tożsame, ujmujące we wszystkich przypadkach całokształt operacji technicznych, jakie można wykonać na danych (od ich utworzenia, poprzez modyfikacje oraz przeniesienia, aż do usunięcia). Na marginesie, zastosowane w tłumaczeniu Decyzji Ramowej określenie „zatajanie", mające stanowić tłumaczenie anglojęzycznego wyrażenia „*suppresing*", w ocenie Autora niniejszej pracy, pozostaje nieadekwatne, sugerując działanie na informacjach nie zaś na danych. Tłumaczenie tego zwrotu, jako „utrudnianie dostępu" nie tylko lepiej koreluje z katalogiem działań wykonywanych na danych, ale obejmuje także wszelkie przypadki utrudnienia dostępu, bez dookreślania jakiejkolwiek formy działania - np. nazywanego zatajaniem. Z uwagi jednak na zapisanie w Decyzji Ramowej poszerzonej przesłanki w brzmieniu „zatajanie lub uczynienie niedostępnymi danych komputerowych", wcześniejsza uwaga dot. samego tłumaczenia zastosowanych zwrotów nie zmienia zakresu samego przepisu. Podobna sytuacja występuje jednak także w tłumaczeniu odnośnego zapisu Dyrektywy, gdzie wyrażenie „*suppresing*" zostało przetłumaczone na język polski, jako „eliminacja". Należy oceniać, iż tak przygotowana transpozycja językowa w istocie zupełnie odbiega od konotacji oryginalnego zwrotu, wprowadzając wyłącznie powtórzenie znamienia „usuwanie".

Na gruncie polskiej ustawy karnej, przestępstwo zakłócania pracy systemu poprzez wykonywanie w nim nieuprawnionych działań zostało stypizowane w aż trzech kolejnych przepisach Kodeksu karnego: art. 268a, 269 oraz 269a.

> „Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych **albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych**, podlega karze pozbawienia wolności do lat 3.
>
> § 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
>
> § 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego
>
> Art. 269. § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo

samorządu terytorialnego **albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych**, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a. Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, **w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej**, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.”.

Rozważania na tle przytoczonych przepisów należy rozpocząć od krytycznego stwierdzenia ich wyraźnie krzyżujących się zakresów przedmiotowych, konstytuujących niejednolitą normę prawną, posługującą się w dodatku niespójną siatką pojęciową. Bezsprzecznie należy podzielić pogląd, że krzyżowanie to stanowi wyraz niskiego poziomu legislacyjnego analizowanej części Kodeksu karnego.

Art. 268a wprowadza w swoim aktualnym brzmieniu penalizację dwóch, w istocie zupełnie różnych czynów[201]:

- czynu bezprawnego niszczenia, uszkadzania, usuwania, zmieniania lub utrudniania dostęp do danych informatycznych, oraz,
- czynu zakłócania lub uniemożliwiania automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych - inaczej niż w przypadku regulacji Konwencji o cyberprzestępczości oraz Decyzji Ramowej, czyn ten nie musi być następstwem żadnych konkretnych operacji na danych (oba stypizowane w przepisie czyny zostały połączone funktorem „albo” wprowadzającym alternatywę rozłączną[202]).

Art. 269 stanowi regulację szczególną wobec art. 268a, zawężając swój zakres przedmiotowy do przestępstw skierowanych przeciwko szczególnej kategorii danych informatycznych *o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego*

---

[201] J. Giezek, op. cit., system LEX - komentarz do art. 268a. k.k.

[202] Zasadne wydaje się zadanie w tym miejscu pytania - czy w świetle zasad logiki prawniczej, czyn, który jednocześnie wypełnia obydwie części przepisu może być ścigany w oparciu o tę jednostkę redakcyjną? Alternatywa rozłączna, symbolizowana w szczególności funktorem „albo” zachowuje swoją prawdziwość wyłącznie w sytuacji, gdy jeden i tylko jeden z jej elementów posiada wartość prawdy.

lub instytucji państwowej albo samorządu terytorialnego. Ponadto, w zakresie penalizacji zakłócania funkcjonowania systemów, poruszany w tym miejscu przepis art. 269 nie wymaga aby zakłócenie nosiło znamię „istotności" (z uwagi na szczególny przedmiot ochrony, ustawodawca uznał, że każdy wpływ na takie dane powinien podlegać karze).

Trzeci z przytoczonych przepisów, art. 269a wprowadził na grunt polskiego Kodeksu karnego regulację odzwierciedlającą wskazane wyżej postanowienia Konwencji o cyberprzestępczości oraz unijnej Decyzji Ramowej, nastawione na zwalczanie przestępstwa zakłócania systemu poprzez wykonywanie w nim nieuprawnionych działań. Inaczej zatem niż w przypadku przepisów art. 268a oraz 269 - traktujących osobno czyny szeroko rozumianej bezprawnej modyfikacji danych informatycznych oraz zaburzania procesów automatycznego przetwarzania danych, przepis art. 269a wprowadził karalność zakłócania pracy systemu POPRZEZ wprowadzenie określonych zmian w stosunku do danych informatycznych.

Analizując znamiona przestępstw zawarte w komentowanych przepisach, zarówno art. 268a, jak i art. 269 posługują się przesłanką „zakłócania lub uniemożliwiania automatycznego przetwarzania, gromadzenia lub przekazywania danych", podczas gdy art. 269a sankcjonuje „zakłócanie pracy systemu komputerowego lub sieci teleinformatycznej". Zastosowanie przez ustawodawcę dwóch różnych sformułowań nakazuje przypisywanie im dwóch różnych znaczeń, choć jak się wydaje - ich istota pozostaje wspólna. Automatyczne przetwarzanie danych obejmuje w istocie całokształt operacji wykonywanych w systemach bowiem każde przetworzenie danych występujących w postaci cyfrowej - czy to zainicjowane bezpośrednim działaniem użytkownika, czy też zaplanowane lub zaprogramowane dużo wcześniej (w tym działania zaprogramowane przez samego autora oprogramowania zainstalowanego w tym systemie - np. systemu operacyjnego), wykonywane jest przez system w sposób „automatyczny". Żadne bowiem z przetworzeń bitów tworzących dane komputerowe, wyrażające się w postaci impulsów elektromagnetycznych, nie może zostać dokonane bezpośrednio przez użytkownika systemu (użytkownik wydaje polecenia, co nie oznacza jednak, że komputer nie przetwarza danych w sposób zautomatyzowany). Jednocześnie, pojęcia „gromadzenia" oraz „przekazywania" danych w istocie zawierają się w najszerszym pojęciu „przetwarzania" danych, a zatem ich odrębne umieszczenie w przepisie należy potraktować, jako wyraz ustawowego *superfluum*. Ustawowa definicja pojęcia „przetwarzanie" zawarta została w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[203], gdzie pojęcie to zostało zdefiniowane (choć w kontekście danych

---

[203] Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.

osobowych, nie zaś danych informatycznych), jako określające „jakiekolwiek" możliwe działania, które mogą zostać wykonane na danych, w tym takie ich zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie [204]. Zakłócanie takiego przetwarzania polega w konsekwencji na wpływaniu na jego zautomatyzowany przebieg, powodując jakiekolwiek zaburzenia normalnej pracy, w szczególności generowanie przez komputer złych wyników, realizowanie działań niezgodnie z wydanymi przez użytkownika poleceniami, czy wreszcie obniżenie wydajności systemu. Pewne wątpliwości mogą pojawić się na tle interpretacji pojęcia „zakłócanie" posiadającego jednoznacznie negatywną konotację. Zadać można zatem pytanie, czy np. przyspieszenie pracy określonego systemu może zostać uznane za jego „zakłócenie"? Z uwagi na przedmiot ochrony, którym *de facto* jest nienaruszalność systemów teleinformatycznych, każdy bezprawny wpływ na pracę systemu powinien być oceniany, jako jego zakłócenie, bowiem ocena rzeczywistych konsekwencji dla danego systemu może nastręczać znacznie więcej trudności, niż samo stwierdzenie zmiany wybranego wskaźnika wydajności (np. razem z poprawą szybkości, może zostać wprowadzona podatność systemu na atak określonego typu). Aby zakłócenie przetwarzania danych, o którym stanowi art. 268a, podlegało kwalifikacji karnej, stopień takiego zakłócenia musi zostać ponadto oceniony, jako „istotny". Za istotne należy uznawać w szczególności takie zakłócenie przetwarzania danych, które wpływa na realizację podstawowych zadań zaatakowanego systemu. To, co jest „istotne" dla pracy jednego systemu, może bowiem pozostawać irrelewantne z punktu widzenia oceny funkcjonalności innego systemu. Kwestia „istotności" winna w efekcie być oceniana zawsze w kontekście konkretnego przypadku[205] - *vide* wcześniejsze uwagi poczynione przy okazji regulacji Konwencji oraz Decyzji Ramowej. Należy ponownie podkreślić, że w przypadku regulacji zawartej w art. 269 Kodeksu karnego - chroniącej dane wrażliwe z punktu widzenia funkcjonowania państwa, kryterium „istotności" zakłócenia nie znajduje zastosowania[206]. Drugie znamię przestępne, którym posługują się przepisy art. 268a oraz 269 Kodeksu karnego - czyli uniemożliwienie przetwarzania danych, oznacza natomiast całkowite wyłączenie wszystkich lub też wybranych funkcjonalności systemu (np. uniemożliwienie samego przekazywania danych poprzez sieci, realizujące przesłankę „uniemożliwienia przetwarzania danych" - należy zwrócić uwagę, że przetwarzaniem danych są jakiekolwiek operacje wykonywane na tych danych).

---

[204] Art. 7 pkt 2 ustawy o ochronie danych osobowych.
[205] Por. M. Siwicki, op. cit., s. 159.
[206] P. Kozłowska-Kalisz, op. cit., system LEX - komentarz do art. 269 k.k.

Inaczej niż w przypadku przepisów art. 268a oraz 269 Kodeksu karnego, art. 269a posługuje się zupełnie inną przesłanką „zakłócenia w istotnym stopniu pracy systemy komputerowego lub sieci teleinformatycznej”. Przesłanka ta nawiązuje bezpośrednio do wskazanych wyżej regulacji Konwencji o cyberprzestępczości oraz Decyzji Ramowej w sprawie ataków na systemy informatyczne, będąc wyrazem bezpośredniej implementacji przepisów o charakterze międzynarodowym do prawa polskiego. Z uwagi na powyższe, do przesłanki tej zastosowanie znajdują wszelkie uwagi poczynione na tle obu wskazanych regulacji prawnych. W tym miejscu, należy jedynie wskazać na wprowadzenie przez ustawodawcę do analizowanego przepisu osobliwego rozróżnienia przedmiotu wykonawczego przestępstwa, na zakłócenie pracy „systemu komputerowego lub sieci teleinformatycznej”. Wprowadzone rozróżnienie, jak również zastosowana do jego budowy siatka terminologiczna nie znajdują obecnie żadnego oparcia w przepisach tzw. prawa informatycznego, bowiem zgodnie z ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadnia publiczne[207], w tej gałęzi polskiego prawa mówi się aktualnie wyłącznie o „systemach teleinformatycznych” (nie zaś komputerowych, czy też informatycznych), w skład którego to pojęcia wchodzą także sieci budowane przez szereg odrębnych systemów. Pojęcie „systemu komputerowego” stanowi bezpośrednie przeszczepienie na grunt prawa polskiego określenia „*computer system*” stosowanego na gruncie postanowień Konwencji o cyberprzestępczości (warto dodać, że Konwencja definiuje to pojęcie - o czym pisano już w poprzednich częściach pracy). Decyzja Ramowa Rady Unii Europejskiej posługuje się natomiast zwrotem „system informatyczny”.

Porównując obie stosowane przez ustawodawcę polskiego przesłanki, to jest: „zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych” oraz przesłankę „zakłócenia pracy systemu komputerowego lub sieci teleinformatycznej”, należy w konsekwencji dojść do wniosku, że pomimo ich zupełnie różnych konstrukcji redakcyjnych, obydwie wskazane przesłanki odwołują się do tego samego stanu faktycznego. Ponieważ cała praca systemów teleinformatycznych polega w istocie na przetwarzania danych w zaprogramowany (czy też zautomatyzowany) sposób - zakłócenie pracy oraz zakłócenie przetwarzania danych stają wyrażeniami synonimicznymi. W tej sytuacji, zastosowanie przez ustawodawcę dwóch różnych wyrażeń na opisanie jednego, tożsamego fragmentu rzeczywistości, należy uznawać za istotny błąd legislacyjny. Błąd ten nakazuje łamać przyjęte zasady interpretacji przepisów

[207] Dz. U. Nr 64, poz. 565, z późn. zm.

prawa, zakładające między innymi konieczność nadawania dwóm różnym zwrotom, dwóch różnych znaczeń. Zasada ta wynika wprost z dogmatu racjonalnego ustawodawcy. Jako wniosek *de lege ferenda* należy wskazać na bezwzględną zasadność dokonania harmonizacji analizowanych przepisów Kodeksu karnego.

Ostatecznie, co było podkreślanie na wstępie niniejszej analizy, art. 269a Kodeksu karnego wprowadza penalizację zakłócenia pracy systemu, która spowodowana została poprzez następujące, bezprawne działania na danych informatycznych:

- ich transmisję,
- zniszczenie,
- usunięcie,
- uszkodzenie,
- utrudnienie dostępu do danych informatycznych, lub też,
- zmianę danych informatycznych.

Powyższy katalog opiera się na rozwiązaniach przyjętych na gruncie Konwencji o cyberprzestępczości, pomijając specyficzną konstrukcję przepisów Decyzji Ramowej. Pomimo bazowania na katalogu Konwencji, w regulacji krajowej pominięto jednak istotne znamię „wprowadzania" danych, które - co warto podkreślić, wymieniane jest jako pierwsze tak w samej Konwencji, jak również Decyzji UE! Brak znamienia wprowadzania danych należy oceniać, jako kolejny, istotny błąd ustawodawcy krajowego. Przypomnijmy - od strony technicznej, po uzyskaniu nieuprawnionego dostępu do systemu, atakujący uzyskuje możliwość wydawania temu systemowi określonych poleceń. Polecenia te wprowadzane są do zaatakowanego systemu w formie odpowiednio przygotowanych komend. Pominięcie przesłanki „wprowadzania danych" oznacza w konsekwencji konieczność kwalifikowania takiego działania, jako nieuprawnionej transmisji danych, stanowiącej swoisty nośnik dla wydawanych komend. Stosując jednak takie rozumowanie, należałoby z przepisu konsekwentnie wyrzucić wszelkie działania oprócz samej transmisji danych, bowiem każda operacja wykonywana w cyberprzestrzeni (poprzez sieci) musi mieć swój ekwiwalent w określonej transmisji danych. Ponownie, należy postulować uzupełnienie sposobu implementacji obowiązujących przepisów międzynarodowych do polskiego systemu prawa.

Wprowadzanie nieuprawnionych zmian danych niepowodujących zakłóceń pracy systemu

Jak zostało zauważone we wstępie do niniejszej części rozdziału, nie wszystkie nieuprawnione działania wykonywane wewnątrz zaatakowanego systemu muszą wywoływać zakłócenia w jego pracy. Ataki, które nie osiągają takiego skutku, ograniczają zakres swojego działania do nieuprawnionych zmian danych, które przetwarzane są w systemie, nie wywołując jednak dalszych konsekwencji dla systemu, jako całości.

Na mocy art. 4 Konwencji Rady Europy o cyberprzestępczości, państwa-strony konwencji zdecydowały się wprowadzić penalizację szeregu nieuprawnionych działań skierowanych przeciwko danym przetwarzanym w systemach teleinformatycznych. Przepis ten - zatytułowany „Zakłócanie danych”[208] (w oficjalnym przekładzie Konwencji „Naruszenie integralności danych”), przyjął następujące brzmienie:

> „Każda ze Stron powinna zastosować takie środki legislacyjne lub inne, które skutkować będą uznaniem za przestępstwo na gruncie jej prawa krajowego, popełnionego umyślnie czynu polegającego na bezprawnym niszczeniu, usuwaniu, uszkadzaniu, modyfikowaniu lub utrudnianiu dostępu do danych komputerowych.”[209]

Ograniczając kontekst niniejszej analizy wyłącznie do cyberprzestępstw, które wykonywane są wewnątrz zaatakowanego systemu, przytoczony przepis stypizował cztery rodzaje operacji wykonywanych wobec danych informatycznych:

- ich niszczenie,
- usuwanie,
- uszkadzanie, oraz
- modyfikowanie.

Jako osobną przesłankę, należy wymienić „utrudnianie dostępu do danych”, które - o czym pisano już wcześniej, stanowi nie tyle rodzaj samodzielnego działania atakującego system, co konsekwencję wprowadzenia określonych zmian w danych informatycznych przetwarzanych w zaatakowanym systemie. Innymi słowy, utrudnienie dostępu do danych stanowi zawsze wynik określonej ingerencji w dane, do których utrudniony ma zostać dostęp lub innych danych, wykorzystywanych do obsługi tego dostępu

[208] W oryginale: „*Data Interference*”. Tłumaczenie własne.

[209] W oryginale: „*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*”. Tłumaczenie własne. W oficjalnym tłumaczeniu Konwencji katalog ten został ujęty, jako „niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych”.

(np. uszkodzenie programu powodujące niemożliwość otworzenia pliku zawierającego dokument tekstowy). W zakresie bliższej charakterystyki samych przesłanek, zastosowanie znajdują w tym miejscu wcześniejsze uwagi, poczynione na tle regulacji art. 5 Konwencji.

Porównując brzmienie komentowanego tu art. 4 oraz wskazanego wyżej art. 5 Konwencji o cyberprzestępczości, warto zauważyć, że przyjęta na gruncie dokumentu budapesztańskiego regulacja karna penalizująca „zakłócanie danych" (a więc zestaw nieuprawnionych czynności dokonywanych wewnątrz systemu, jednak nie zakłócających jego ogólnej pracy) została sformułowana z pominięciem dwóch istotnych przesłanek opisujących metodę popełnienia cyberataku, tj. - „poprzez transmisję" oraz „poprzez wprowadzenie danych". Zidentyfikowana różnica redakcyjna uprawnia podniesienie dwóch następujących wątpliwości natury legislacyjnej:

- po pierwsze, brak przesłanki „działania poprzez transmisję danych" może stanowić podstawę do rozważań, czy czyn typizowany w art. 4 Konwencji w istocie może być popełniony za pośrednictwem sieci, czy też wyłącznie lokalnie (przez cyberprzestępcę siadającego bezpośrednio przed atakowanym komputerem). Wątpliwość ta rysuje się na tle różnic redakcyjnych dwóch wskazanych przepisów Konwencji, które to różnice - zgodnie z przyjętymi zasadami interpretacji przepisów prawa, należy odczytywać, jako intencjonalne zróżnicowanie treści wskazanych norm prawnych,
- po drugie zaś, brak przesłanki „działania poprzez wprowadzanie danych" występującej w art. 5 Konwencji, powoduje wątpliwości, czy stypizowane w art. 4 zakłócenie danych informatycznych może polegać np. na ich uszkodzeniu poprzez dopisanie do kodu źródłowego zaatakowanego pliku dodatkowych linijek. Co istotne, nie każde nieuprawnione „powiększenie" pliku będzie powodować jego dysfunkcję, choć niewątpliwie stanowi formę nieuprawnionej ingerencji w dane informatyczne.

Próbując udzielić na powyższe pytania należy stwierdzić, że przepis art. 4 penalizuje między innymi każdą nieuprawnioną modyfikację danych, co więcej, bez znaczenia w jaki sposób modyfikacja ta została dokonana. Tym samym, sposób działania sprawcy cyberataku pozostaje w istocie bez znaczenia dla możliwości zakwalifikowania jego działania, jako spowodowania nieuprawnionej modyfikacji danych w systemie. Z uwagi jednak na rangę Konwencji o cyberprzestępczości, wskazaną niespójność redakcyjną należy ocenić, jako istotny błąd o charakterze legislacyjnym.

Analogiczna regulacja penalizująca dokonywanie nieuprawnionych działań wewnątrz systemu, nie powodujących zakłóceń jego pracy, zawarta została także w art. 4 Decyzji

Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[210]. Przepis ten otrzymał brzmienie:

> „Każde Państwo Członkowskie podejmuje niezbędne środki celem zapewnienia, że umyślne bezprawne usunięcie, uszkodzenie, pogorszenie, zmiana, zatajanie lub uczynienie niedostępnymi danych komputerowych w systemie informatycznym jest karane jako przestępstwo, kiedy dokonywane jest bezprawnie, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.”.

W zastępującej przytaczaną Decyzję Dyrektywie Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne[211] - typizacja czynu bezprawnej ingerencji w dane przybrała natomiast postać przepisu o treści:

> „Artykuł 5 Niezgodna z prawem ingerencja w dane
>
> Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi, było karalne jako przestępstwo, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.”

Zgodnie z redakcjami przytoczonych przepisów, w ich treści stypizowane zostały działania polegające na bezprawnym:

- usunięciu,
- uszkodzeniu,
- pogorszeniu,
- zmienieniu,
- zatajeniu / eliminowaniu (zmiana wynikająca z różnić w tłumaczeniu wyrazu „*suppressing*” – kwestia poruszana już kilkukrotnie na gruncie niniejszego rozdziału), lub też,
- uczynieniu niedostępnymi

danych komputerowych.

Tak samo, jak w przypadku zapisu art. 4 Konwencji o cyberprzestępczości, również art. 4 Decyzji Ramowej oraz art. 5 Dyrektywy również nie wskazały w swojej redakcji na przesłanki działania poprzez transmisję danych, jak również działania poprzez wprowadzenie

---

210 Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW.

211 Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

danych. Ponownie jednak, z uwagi na zawarcie w przepisach przesłanki odnoszącej się do penalizacji wszelkich nieuprawnionych modyfikacji danych przetwarzanych w systemie (określone mianem „zmienianie”), praktyczne zastosowanie przepisów wobec przypadków modyfikacji danych za pośrednictwem sieci, jak również modyfikacji danych poprzez ich nieuprawnione „uzupełnienie”, nie budzą wątpliwości natury praktycznej. Zastosowana przez autorów Decyzji „automatyka” w powtarzaniu rozwiązań przyjętych na gruncie Konwencji oraz stanowiąca jej następstwo – automatyka w budowaniu (a w istocie powtarzaniu) postanowień Dyrektywy, zasługuje jednak na krytyczną uwagę.

Za wyjątkiem przesłanki „pogorszenia danych”, pozostałe przesłanki wymienione w art. 4 Decyzji oraz art. 5 Dyrektywy były już przedmiotem rozważań w poprzedniej części pracy, w ramach analizy sposobu sankcjonowania nieuprawnionych działań wywołujących zakłócenia w pracy systemu. Przesłankę „pogorszenia danych” należy odnosić do takiego zmodyfikowania danych, które nie powoduje niemożliwości ich jakiegokolwiek wykorzystania, lecz obniża ich wartość, czy też funkcjonalność. Pogorszeniem danych może być np. proste usunięcie przygotowanej edycji dokumentu, powodujące choćby zlanie całego tekstu w jedną całość, bez odstępów, tytułów, itd. O ile działanie takie nie usuwa żadnych treści, o tyle czyni zaatakowane dane wysoce uciążliwymi do dalszego przetwarzania. Znaczeniu przytoczonej przesłanki nie należy jednak przypisywać istotnej roli w budowie komentowanych przepisów, ponieważ z praktycznego punktu widzenia, najważniejsze jest ujęcie w ich redakcji najszerszego znamienia „zmieniania danych”. Każda operacja na danych komputerowych, czy to polegająca na ich częściowym lub całościowym usunięciu, nadpisaniu, zmodyfikowaniu, czy pogorszeniu, mieści się bowiem w zakresie przedmiotowym pojęcia bezprawnej „zmiany danych”, a zatem stanowi tylko jeden z elementów szeroko rozumianego zmieniania, czy też modyfikowania danych.

Na gruncie prawa polskiego, nieuprawnione wprowadzanie w systemie zmian niepowodujących zakłócenia jego pracy, ujęte zostało aż w trzech przepisach Kodeksu karnego. Przepisami tymi są art. 268, 268a oraz 269 Kk:

„Art. 268. § 1. Kto, nie będąc do tego uprawnionym, **niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, **niszczy, uszkadza, usuwa,**

zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

Art. 269. § 1. Kto **niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego** albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.”.

Zgodnie z przytoczonymi jednostkami redakcyjnymi, w polskim porządku prawnym, w sposób niezależny spenalizowane zostały działania polegające na:

- udaremnianiu lub znacznym utrudnianiu osobie uprawnionej zapoznanie się z istotną informacją, dokonywane w szczególności - ale nie tylko, poprzez niszczenie, uszkadzanie, usuwanie lub zmienianie zapisu takiej informacji,
- niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostęp do danych informatycznych, oraz
- niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu danych informatycznych o szczególnym znaczeniu dla obronności kraju [...].

W pierwszej kolejności należy podkreślić, że podczas, gdy regulacja art. 268 Kodeksu karnego odnosi się do ochrony „zapisu istotnej informacji”, przedmiotem ochrony przepisów art. 268a oraz 269 Kk są dane informatyczne. Rozróżnienie to wymaga odrębnego potraktowania, bowiem inaczej niż w przypadku analizowanego w pierwszej części rozdziału art. 267 Kk, komentowany w tym miejscu przepis art. 268 Kk posługuje się nie tyle kategorią „informacji”, co „zapisu informacji”. Stosując wielokrotnie już przywoływaną zasadę racjonalnego ustawodawcy, należy uznać, że obydwa wskazane zwroty mają swoje, odrębne znaczenie. O ile zatem „informacją” w cyberprzestrzeni są przede wszystkim treści komunikowane użytkownikowi w ramach wykonywanego ruchu sieciowego, wyrażenie „zapis informacji” należy - w ocenie autora niniejszej pracy, odnosić do aspektów technicznych, odzwierciedlających same zasady budowy informacji w cyberprzestrzeni. Cała cyberprzestrzeń zbudowana jest z niekończących się ciągów bitów, czyli logicznych zer i jedynek. Bity te tworzą następnie „dane informatyczne”, czy też „dane komputerowe”, reprezentujące wszelkie procesy oraz zasoby, które są wykonywane lub przetwarzane w systemach teleinformatycznych. Niektóre z danych tworzą zapis informacji - np. dane pliku

dokumentu tekstowego. Inne zaś, pełnią inne funkcje, nie składając się na informacje czytelne dla użytkownika. W związku z powyższym, zasadne wydaje się stwierdzenie, że pojęcie „zapisu istotnej informacji" odnosi się *de facto* do danych informatycznych, które pełnią pierwszą z wymienionych ról, tzn. tworzą informacje. Przedmiotem ochrony z art. 268 Kodeksu karnego nie jest zatem sama informacja, zaś dane, które ją budują.

Po drugie, należy zaznaczyć, że art. 268 Kodeksu karnego penalizuje nie tyle samo „niszczenie, uszkadzanie, usuwanie lub zmienianie" informacji, co udaremnianie lub znaczne utrudnianie zapoznania się z informacją osobie uprawnionej. Wskazane wcześniej znamiona sprawcze należy zatem rozumieć, jako przykładowe działania techniczne, służące do osiągnięcia celu w postaci ograniczenia dostępu osoby uprawnionej do określonej informacji. Konstrukcja ta w sposób wyraźny różni się od postanowień przyjętych na gruncie tak Konwencji o cyberprzestępczości, jak i Decyzji Ramowej UE, gdzie posługiwano się wyłącznie określeniem szeroko rozumianej „modyfikacji" danych. Regulacja krajowa - dla uznania karalności określonego czynu, wymaga zatem dokonania ustalenia, czy wprowadzone zmiany spełniły przesłankę „udaremnienia lub znacznego utrudnienia" dostępu do informacji, którą należy oceniać, jako zawężającą zakres wprowadzonej przez ustawodawcę ochrony prawnej. Należy zaznaczyć, że wskazane wcześniej regulacje międzynarodowe wprowadzały proste kryteria karalności samej zmiany danych, pozostawiając poza oceną prawną kwestie skutków, jakie zmiany te powodują wobec dostępności danych, czy też jeszcze węziej - dostępności informacji.

Po trzecie zaś, jak wynika z redakcji art. 268 Kodeksu karnego, przepis ten chroni zapis wyłącznie informacji „istotnej". Niestety, ustawodawca nie udzielił osobom stosującym prawo żadnych wskazówek, co do przeprowadzania kwantyfikacji informacji, jako „istotnej", pozostawiając tę ocenę *de facto* uznaniu sądu. Ocena „istotności" powinna być dokonywana w szczególności z zachowaniem kryteriów obiektywnych, jak i subiektywnych, to jest z uwzględnieniem wartości informacji tak dla przeciętnego użytkownika danej informacji, jak i skonkretyzowanej osoby uprawnionej do zapoznania się z nią. Należy oceniać, że wprowadzenie do analizowanego przepisu nieostrego kryterium „istotności" informacji nie spełnia postulatu jednoznaczności prawa, tak przecież istotnego w gałęzi prawa karnego[212].

Jak zostało zauważone powyżej, art. 268a oraz 269 Kodeksu karnego wprowadzają do polskiej ustawy karnej ochronę „danych informatycznych". Art. 269 stanowi tu regulację szczególną, nastawioną na ochronę określonej kategorii danych, choć przy istotnym

[212] Por. M. Siwicki, op. cit, s. 157 i nast.

ograniczeniu tej ochrony - o czym szerzej nieco dalej. W kontekście penalizacji wykonywania nieuprawnionych zmian wewnątrz systemu, art. 268a Kk typizuje szereg działań polegających na „niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostęp do danych informatycznych". Z praktycznego punktu widzenia, najistotniejszym znamieniem przestępstwa opisanego w przepisie jest samo „zmienianie" danych, bowiem każda ingerencja w dane spełnia tę przesłankę (tak uszkadzanie, nadpisywanie, uzupełnianie, jak i usuwanie wiążą się z dokonywaniem nieuprawnionych „zmian" danych). Przesłanka „utrudniania dostępu do danych" wprowadza natomiast karalność czynów polegających na atakowaniu danych innych, niż te do których ograniczony zostanie dostęp - np. danych budujących program komputerowy służący do otwierania plików określonego rodzaju (taki atak nie dotyka w żadnej mierze samych danych, do których utracony zostaje dostęp). W tym kontekście, na szczególne podkreślenie zasługuje fakt, iż przesłanka „utrudniania dostępu do danych" została pominięta w art. 269 Kodeksu karnego, który to przepis zapewnia szczególną ochronę danych o istotnym znaczeniu dla funkcjonowania państwa („dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego"). Brak powyższej przesłanki oznacza intencjonalne ograniczenie przez ustawodawcę zakresu ochrony informacji wrażliwych dla państwa, co wydaje się być pozbawione jakiegokolwiek uzasadnienia faktycznego. Niefortunną redakcję przepisu art. 269 Kk ratuje w pewnym sensie druga część komentowanego przepisu, odnosząca się do przestępstwa zakłócania funkcjonowania systemu teleinformatycznego (czyn ten analizowany był w poprzedniej części rozdziału). Należy uznać, że przestępstwa polegające na „utrudnianiu dostępu do danych" w istocie poddają się subsumcji pod regulacje karne penalizujące „zakłócanie automatycznego przetwarzania danych".

§5. Oszustwo komputerowe

Z punktu widzenia analizy zjawiska nowoczesnej przestępczości komputerowej, niezwykle interesującym cyberprzestępstwem jest tzw. oszustwo komputerowe. Czyn ten, łącząc w sobie elementy nieuprawnionych działań o charakterze technicznym, z elementami socjotechniki oraz inżynierii społecznej, stanowi jeden z najczytelniejszych przykładów, w jaki sposób cyberprzestrzeń zmieniła postrzeganie znanych już zjawisk przestępczych

- w tym wypadku klasycznego oszustwa[213]. Warto od razu zaznaczyć, że dla uznania danego czynu za oszustwo komputerowe niezbędne jest łączne wystąpienie dwóch wskazanych wyżej elementów - to jest nieuprawnionego działania technicznego oraz wprowadzenia użytkownika systemu w błąd. Czyn, który dokonywany jest za pośrednictwem sieci komputerowych, jednak nie zawiera w swoim opisie stanu faktycznego żadnych bezprawnych czynności technicznych, należy kwalifikować, jako zwykłe oszustwo - np. podanie przez nieuczciwego pracownika własnego numeru konta do dokonania przelewu na rzecz zatrudniającej go firmy, nie staje się oszustwem komputerowym nawet w przypadku, gdy sam przelew dokonywany jest *on-line* za pośrednictwem internetowej usługi bankowej.

Istotą oszustwa komputerowego jest zastosowanie technik informatycznych w taki sposób, aby wprowadzić użytkownika systemu w zamierzony błąd, a następnie błąd ten wyzyskać dla osiągnięcia określonego celu[214]. Cel ten może przybierać bardzo zróżnicowane formy. Do najbardziej typowych skutków oszustwa komputerowego należy zaliczyć[215]:

- wyłudzenie danych osobowych,
- wyłudzenie haseł dostępowych do najróżniejszych usług sieciowych - tzw. *phishing,*
- podsłuchiwanie transmisji danych,
- spowodowanie wykonania przez użytkownika systemu określonej czynności faktycznej - np. dokonania przelewu bankowego na nieprawdziwy numer konta widniejący na przerobionej stronie internetowej (stronie poddanej tzw. atakowi *deface*),
- wprowadzenie do systemu ofiary oprogramowania złośliwego, które ofiara akceptuje błędnie sądząc, że zgadza się np. na zainstalowanie darmowego oprogramowania antywirusowego, czy też wreszcie,
- włączenie komputera ofiary do sieci komputerów *zombie,* czyli tzw. *botnetu,* który następnie wykorzystywany jest przez zorganizowane grupy przestępcze do popełniania najpoważniejszych cyberataków.

Powyższy katalog celów oszustów komputerowych nie jest oczywiście zamknięty. Co więcej, wraz z rozwojem nowoczesnych technologii, jego zakres przedmiotowy ulega poszerzeniu o ataki skierowane na nowe rodzaje usług świadczonych w cyberprzestrzeni.

---

[213] T. Trejderowski, Kradzież tożsamości. Terroryzm informatyczny, Eneteia, Warszawa 2013, s. 11 i nast.

[214] *Ibidem,* s. 11 - 15.

[215] Wykorzystano uwagi zawarte w: M. Kliś, op.cit. oraz A. Kania, Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni, *e-biuletyn* CBKE 1/2009, Wrocław 2009, s. 12 i nast., tekst opracowania dostępny na stronie internetowej pod adresem: http://bibliotekacyfrowa.pl/Content/34350/Oszustwo_komputerowe.pdf, a także T. Trejderowski, op. cit., s. 14 i nast.

Jedną z podstawowych metod przeprowadzania oszustwa komputerowego jest stosowanie tzw. inżynierii społecznej (z ang. *social engineering*[216]). Metoda ta opiera się na prostym założeniu, że nierzadko łatwiej jest wykorzystać ludzką niewiedzę, czy też naiwność, niż łamać nowoczesne zabezpieczenia teleinformatyczne. Jak zaznaczał K. Mitnick[217] - jeden z największych oszustów komputerowych wszechczasów, aktualnie uznany konsultant bezpieczeństwa systemów teleinformatycznych, nie ma sensu łamać haseł do komputerów, skoro można poprosić o nie ich użytkowników[218]. Istotą komputerowej inżynierii społecznej jest bowiem dokonanie określonej manipulacji na ludziach - podszycie się pod inną osobę, wprowadzenie użytkownika systemu w błąd oraz ostatecznie - nakłonienie go do dobrowolnego poddania się oszustwu. O ile element te charakteryzują także klasyczne oszustwo, w przypadku cyberprzestępczości, działania te przybierają wyrafinowaną formę techniczną.

Z punktu widzenia technicznego, typowymi sposobami działania cyber-oszustów jest przygotowywanie wiadomości e-mail, czy też witryn internetowych, które swoim wyglądem przypominają strony lub też pocztę banków internetowych. Skopiowanie oryginalnej szaty graficznej strony WWW nie wymaga praktycznie żadnej wiedzy specjalistycznej z zakresu teleinformatyki. Jeżeli zatem użytkownik nie zorientuje się, że adres internetowy jego banku uległ choćby kosmetycznej „zmianie" (np. zamiast www.nazwabanku.pl - www.nazwa-banku.pl, czy też www.nazwabanku.e-usługi.pl), jest w stanie wpisać swoje poufne dane - login i hasło, na stronie oszusta. Skorzystanie z takiej „podmienionej" strony jest natomiast często wynikiem rozsyłania spreparowanych wiadomości poczty elektronicznej, proszących np. o dokonanie aktualizacji konta bankowego w związku z migracją danych na nowy serwer. Wiadomości takie zawierają następnie wygodny odsyłacz do strony „banku". Dla ukrycia przestępnego działania, użytkownik - po podaniu swoich danych uwierzytelniających go w systemie, otrzymuje podziękowanie za pomyślne przeprowadzenie czynności oraz zostaje przekierowany na prawdziwą stronę banku, gdzie może sprawdzić, że cała usługa rzeczywiście działa bez zarzutów.

Ponieważ przygotowanie skutecznego oszustwa często wymaga pozyskania określonej wiedzy - np. adresów e-mail klientów danego banku, inżynieria społeczna często poprzedzana

[216] Por. W. Gragido, J. Pirc, *Cybercrime and Espionage. An analysis of Subversive Multivector Threats,* Elsevier, USA 2011, s. 68 i nast. Nazwa ta stosowana jest także powszechnie w biuletynach bezpieczeństwa największych firm komputerowych, tak np. na stronie internetowej dostępnej pod adresem: http://www.microsoft.com/security/resources/socialengineering-whatis.aspx.

[217] Więcej na temat jego osoby na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Kevin_Mitnick.

[218] K. Mitnick poświęcił temu zagadnieniu napisaną przez siebie książkę pod tytułem „Sztuka podstępu". Jej mottem stało się zdanie „Łamałem ludzi, nie hasła".

jest innymi atakami o charakterze *stricte* technicznym, np. atakami mającymi na celu uzyskanie nieuprawnionego dostępu do systemu oraz wykradzenie z niego interesujących informacji. Co ciekawe, źródłem istotnych danych mogą być także np. wydruki z systemów, które nierozważnie wyrzucane są często jako zwykłe śmiecie. Przeglądanie śmietników dużych korporacji w celu znalezienia informacji o charakterze technicznym otrzymało nawet swoją nazwę „śmietnikowego nurkowania" (z ang. „*dumpster diving*"[219]).

Na gruncie polskiego prawa karnego, oszustwo komputerowe spenalizowane zostało na podstawie art. 287 Kodeksu karnego. Przepis ten stanowi, że:

> „Art. 287. § 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
>
> § 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
>
> § 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego."

Zgodnie z przytoczonym § 1 art. 287 Kk, na mocy polskiej ustawy zabronione jest:

- nieupoważnione wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych, jak również,
- nieupoważnione zmienianie, usuwanie albo wprowadzanie nowego zapisu danych informatycznych

o ile działania te dokonywane są w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody. Tym samym, jak zauważa się w piśmiennictwie, tak stypizowanym oszustwem nie będą czyny powodowane np. chęcią samo-dowartościowania się sprawcy[220], pod warunkiem jednak, iż nie będą powodować szkód wobec osób trzecich[221].

Pośród istotnych cech komentowanego przepisu należy wskazać następujące elementy:

---

[219] M. Cross, D. Littlejohn Shinder, *Scene of the Cybercrime*, Syngress 2008, s. 491.

[220] Por. A. Kania, Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni, *e-biuletyn* CBKE 1/2009, Wrocław 2009, s. 4, tekst opracowania dostępny jest na stronie internetowej pod adresem: http://bibliotekacyfrowa.pl/Content/34350/Oszustwo_komputerowe.pdf

[221] Należy zaznaczyć, iż przyjęta konstrukcja przepisu dopuszcza także możliwość ujęcia szkody powstałej po stronie podmiotów świadczących określone usługi sieciowe (np. *hosting*) wykorzystywane w ramach popełnienia przestępstwa oszustwa komputerowego – w tym np. szkody wizerunkowe obniżające wartość przedsiębiorstwa.

- art. 287 Kk obejmuje swoją ochroną dane informatyczne oraz procesy ich automatycznego przetwarzania. W tym sensie, charakter przepisu zbliża się do regulacji art. 268a orz 269 Kk, które również identyfikowały swój przedmiot ochrony poprzez odniesienie do danych, nie zaś informacji, jak czyni to art. 267 Kk, czy też zapisu informacji, jak w art. 268 Kk,
- to, co w istotnym stopniu odróżnia art. 287 Kk od art. 268a Kk to zastosowanie w art. 287 Kk znamienia „wpływania na automatyczne przetwarzanie danych", które zastąpiło znane z analizowanych wcześniej regulacji znamię „zakłócania automatycznego przetwarzania danych". Oszustwo komputerowe nie polega zatem - zgodnie z przyjętą redakcją przepisu, na zakłóceniu funkcjonowania systemu, co na osobliwym wpłynięciu na to funkcjonowanie, tak by dokonać manipulacji na jego użytkowniku. Warto jednak w tym miejscu zauważyć, że od strony technicznej, każde wpłynięcie na pracę systemu oznacza jednoczesne zakłócenie jego *oryginalnej* pracy. W tym sensie, przepis art. 287 Kodeksu karnego należy traktować, jako *lex specialis* wobec innych regulacji karnych, również odnoszących się do zaburzania pracy systemu. Jednocześnie, nie każde „wpłynięcie" na pracę systemu, musi koniecznie oznaczać jego „zakłócenie",
- § 1 art. 287 Kk sformułowany został z zastosowaniem alternatywy łącznej (lub), spajającej znamiona „wpływania" na szeroko pojętą pracę systemu oraz „zmiany, usuwania albo wprowadzania danych informatycznych". Oznacza to, że przepis ten występuje w faktycznym zbiegu z regulacjami art. 268, 268a oraz 269 Kk, typizującymi działania polegające na uszkadzaniu treści zapisanych wewnątrz atakowanego systemu. Zbiegu tego nie eliminuje fakt uczynienia z art. 287 Kk przepisu skutkowego („w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody"), bowiem *de facto* każde uszkodzenie danych należących do innej osoby powoduje po jej stronie wystąpienie szkody. Jednocześnie, ponieważ art. 287 odnosi się do najszerszego kryterium ochrony „danych informatycznych", jego zakres przedmiotowy obejmuje tym bardziej dane istotne dla kraju, jak również zapis istotnej informacji, o których stanowią odpowiednio art. 269 oraz 268 Kk.

Powyższa charakterystyka legislacyjna nie pozwala wyrazić jednoznacznej aprobaty dla redakcji art. 287 Kodeksu karnego. Nieostre znamię „wpływania" na procesy, jak również brak wyraźnego rozgraniczenia celu regulacji od przepisów art. 268 - 269 Kk, świadczą bez wątpienia o niskim poziomie merytorycznym przepisu. Sytuacja ta z pewnością wynika

w dużej mierze z braku jednolitych standardów międzynarodowych, które regulowałyby karalność oszustwa komputerowego. Czyn taki nie został zdefiniowany ani w Konwencji o cyberprzestępczości, ani również wielokrotnie przywoływanej Decyzji Ramowej Rady Unii Europejskiej w sprawie ataków na systemy informatyczne, czy wreszcie Dyrektywie Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne.

Rozdział V

Dowód elektroniczny - charakterystyka oraz klasyfikacja śladów cyberprzestępstw

Niniejszy rozdział pracy, otwierający część procesową całego opracowania, poświęcony został próbie zbudowania definicji pojęcia „dowodu elektronicznego". I choć podobnie, jak w przypadku charakteryzowania cyberprzestępczości, także i dowód elektroniczny nie stanowi w obecnym stanie prawnym kategorii ustawowej[1] (termin ten nie należy do zasobu języka prawnego, zaś prawniczego - to jest języka II stopnia), jego przybliżenie oraz poprawne zrozumienie nie tylko pozwala w sposób istotny uzupełnić obraz zjawiska cyberprzestępczości, ale przede wszystkim zaprezentować współczesne wyzwania procesu karnego, związane z podejmowaniem czynności procesowych nakierowanych na wykrycie oraz opisanie zaistniałego czynu bezprawnego popełnionego w cyberprzestrzeni[2]. Warto również dodać, że wedle aktualnych szacunków, ponad 99% informacji, wytwarzanych jest na świecie właśnie w formie elektronicznej[3], budując tym samym ogromny zasób potencjalnego materiału dowodowego, którego znaczenia - szczególnie w dobie informatyzacji, nie można przecenić[4].

Realizując zakreślone powyżej cele rozdziału, niniejsza część pracy porusza kolejno następujące zagadnienia:

I. co oznacza samo pojęcie „dowodu elektronicznego"?,

II. jakie są inne określenia używane w odniesieniu do śladów pozostawianych w toku popełniania cyberprzestępstw?,

---

[1] B. Fischer, Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalisytczne, Zakamycze, Kraków 2000, s. 113.

[2] Aspekt ten podkreśla A.Lach w: Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia teoretyczne i praktyczne, *e-biuletyn* CBKE 2/2004, Wrocław 2004, s. 1. Tekst opracowania dostępny jest na stronie internetowej pod adresem: http://www.bibliotekacyfrowa.pl/Content/24720/Dowody_cyfrowe_w_postepowan.pdf.

[3] M. C. S. Lange, K. M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know*, Wydawnictwo American Bar Association, Chicago 2009, s. 2.

[4] K. J. Pawelec, Proces dowodzenia w postępowaniu karnym, Lexis Nexis, Warszawa 2010, s. 24. Autor zwraca szczególną uwagę na powszechność występowania dowodów elektronicznych we współczesnej rzeczywistości społeczeństwa informacyjnego.

III. czym są informatyczne nośniki danych?,

IV. czym w istocie jest dowód elektroniczny (ze szczególnym uwzględnieniem charakterystyki tzw. dokumentu elektronicznego) oraz jakim klasyfikacjom można go poddać?,

V. jaki stosunek - w przypadku cyberprzestępczości, zachodzi pomiędzy dowodem przestępstwa, a faktycznym narzędziem jego popełnienia?, i wreszcie,

VI. gdzie należy szukać dowodów elektronicznych?

Z racji na konieczność otwarcia rozdziału na zagadnienia wykraczające poza ramy *stricte* prawne, prowadzone w nim rozważania w dużej mierze wykorzystują informacje zawarte w rozdziale III pracy - zatytułowanym *Technologia cyberprzestrzeni*. Informacje te, dla uniknięcia powtórzeń, nie będą ponownie przedstawiane, zaś jedynie rozszerzane tam, gdzie jest to zasadne dla uzupełnienia kontekstu faktycznego występowania dowodów elektronicznych. Z uwagi na wciąż skąpą liczbę prawdziwie analitycznych opracowań krajowych poświęconych tematyce dowodu elektronicznego - pośród których wyróżnić należy prace prof. A. Adamskiego[5], dr. A Lacha[6], czy też W. Kasprzaka[7], rozważania zawarte w niniejszym rozdziale uzupełniane są zagranicznym dorobkiem prawnym oraz prawniczym.

§1. Znaczenie pojęcia „dowód elektroniczny"

Jak zostało zauważone na wstępie, wyrażenie „dowód elektroniczny" nie stanowi w obecnym, obowiązującym w Polsce stanie prawnym, pojęcia ustawowego oraz nie posiada swojej definicji legalnej, stanowiąc szczególny rodzaj dowodu w ujęciu klasycznym[8]. W doktrynie krajowej podkreśla się w szczególności, że mianem dowodu elektronicznego powinno określać się:

„informację w formie elektronicznej o znaczeniu dowodowym"[9],

czy też,

„dane stanowiące materiał dowodowy" w sprawach o przestępstwa popełniane

---

5 Np. A. Adamski, Prawo karne komputerowe, CH Beck, Warszawa 2000, czy A. Adamski, Przestępczość w cyberprzestrzeni, prawne środki przeciwdziałania zjawiska w Polsce na tle projektu konwencji Rady Europy, Dom Organizatora, Toruń 2011.

6 Np. A. Lach, Dowody elektroniczne w procesie karnym, Towarzystwo Naukowe Organizacji i Kierownictwa, Dom Organizatora, Toruń 2004, czy A.Lach, Dowody cyfrowe..., op. cit.

7 W. Kasprzak, Ślady cyfrowe. Studium prawno-kryminalistyczne, Difin, Warszawa 2015.

8 Więcej na temat definicji ogólnych oraz klasyfikacji dowodów w ujęciu klasycznym w: A. Gaberle, op. cit., S. Waltoś, Proces karny. Zarys systemu, Lexis Nexis, Warszawa 2009, wyd. 10, czy T. Grzegorczyk, J. Tylman, Polskie postępowanie karne, Lexis Nexis, Warszawa 2011, wyd. 8.

9 A. Lach, Dowody elektroniczne..., op. cit., s. 28.

z wykorzystaniem technologii informacyjnych[10].

Podobne rozumienie dowodu elektronicznego - jako formy szczególnego środka dowodowego, prezentowane jest także w bogatej w tym zakresie literaturze amerykańskiej[11], gdzie pojęcie „dowodu elektronicznego" definiowane jest przykładowo, jako:

> „wszelkie dane przechowywane lub przekazywane z wykorzystaniem komputera, które wspierają, bądź też obalają teorię opisującą w jaki sposób nastąpiło przestępstwo lub też które dotykają istotnych elementów przestępstwa, takich jak zamiar, czy alibi"[12],
>
> „każdy dowód, którego istnienie oparte jest na technologii, bez względu na sposób jego pozyskania, czy też cel zastosowania"[13],

jak również:

> „informacja oraz dane o wartości śledczej, które są przechowywane lub przekazywane z użyciem komputera"[14].

Pojęcie „dowodu elektronicznego" obecne jest także w dokumentach Unii Europejskiej, choć na gruncie tym występuje niestety bez swojej definicji legalnej. Przykładowo, kwestie konieczności usprawnienia procedur pozyskiwania „dowodów elektronicznych" - w tym w ramach międzynarodowej pomocy prawnej, poruszane były w komunikacie Komisji z 2000 r., zatytułowanym „Tworzenie bezpieczniejszego społeczeństwa informacyjnego poprzez podwyższanie poziomu bezpieczeństwa infrastruktury informacyjnej oraz zwalczanie przestępczości związanej z komputerami"[15], czy też komunikacie Komisji z 2007 r., zatytułowanym „W kierunku wytworzenia polityki w sprawie zwalczania cyberprzestępczości"[16].

Cechą wspólną przytaczanych wyżej definicji jest utożsamianie dowodu elektronicznego z dowodem w rozumieniu środka dowodowego[17], mogącego stanowić

---

10 A. Adamski, Prawo karne..., op. cit., s. 192.

11 Tak np. M. C. S. Lange, K. M. Nimsger, op cit, E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Elsevier, Massachusetts 2011, czy też A. M. Gahtan, *Electronic Evidence*, Carswell 1999 - ostatni tytuł przytaczam za: A. Lach, Dowody elektroniczne op. cit., s. 28.

12 E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Elsevier, Massachusetts 2011, s. 7.

13 Michele C. S. Lange, Kristin M. Nimsger, op. cit., s. 4.

14 Definicja amerykańskiego Związku Komendantów Policji, przytaczam za: E. Casey, op. cit., s. 7.

15 Tytuł oryginalny: „*Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime.*" Tłumaczenie własne. Pełny tekst komunikatu dostępny na stronie internetowej pod adresem: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0890:EN:HTML.

16 Tytuł oryginalny: „*Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime*". Tłumaczenie własne. Pełny tekst komunikatu dostępny na stronie internetowej pod adresem: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:EN:HTML.

17 Jedno z klasycznych sposobów pojmowania pojęcia „dowodu". Tak np. T. Grzegorczyk, Dowody w procesie

materiał w sprawie karnej (wyraźne odwołanie do dowodu w ujęciu klasycznym[18]). Nie jest to zatem dowód w rozumieniu np. procesu badawczego, procesu rozumowania logicznego, czy też źródła poznania (jak np. świadek w opozycji do zeznania). Obok zaznaczonej cechy wspólnej, przytoczone definicje pozwalają jednak także wskazać istotną różnicę w sposobie definiowania pojęcia „dowodu elektronicznego" wyrażającą się w alternatywnym przyjmowaniu za *genus* definicji bądź to wartości „informacji", bądź też „danych". Różnica ta wyraźnie zarysowuje się w szczególności na tle porównania dwóch przytoczonych wyżej definicji autorów krajowych.

Powyższa kwestia wymaga nieco bliższego przyjrzenia się znaczeniom pojęć „informacja" oraz „dane" - w szczególności w odniesieniu do stosowania tych wyrażeń na gruncie szeroko rozumianej teleinformatyki. I tak, zgodnie z wpisem pochodzącym z internetowej wersji encyklopedii PWN, mianem informacji określa się „wyobrażenie, wyjaśnienie, zawiadomienie", choć jednocześnie encyklopedia uzupełnia przedstawioną typologię stwierdzeniem, że termin ten jest „w zasadzie niedefiniowalny"[19]. Owa niedefiniowalność wynika z traktowania „informacji", jako pojęcia podstawowego, porównywalnego np. do pojęcia energii. W kryminalistyce, pod pojęciem „informacji„ rozumie się między innymi „wszelkie dane o świecie zewnętrznym, które uzyskujemy przez bezpośrednie poznanie zmysłowe, albo przez podawany przez inną osobę opis jakiegoś zjawiska lub rzeczy"[20]. W cybernetyce natomiast - a więc obszarze funkcjonowania technicznego języka specjalistycznego, informację definiuje się przykładowo, jako „związek między stanami tego samego zbioru"[21] - a więc np. związek pomiędzy badanym ciśnieniem atmosferycznym, a wynikiem pomiaru dokonywanego z zastosowaniem określonej jednostki miary. Ostatecznie, w ujęciu potocznym, słownik języka polskiego PWN, nakazuje pod pojęciem „informacji" rozumieć: „1 wiadomość o czymś lub zakomunikowanie czegoś; 2 dział informacyjny urzędu, instytucji; 3 **dane** przetwarzane przez komputer"[22] (podkreślenie własne).

W najszerszym ujęciu, „dane" to wszelkie przejawy rzeczywistości, które tylko mogą

karnym, Wydawnictwo Prawnicze, Warszawa, 1998, s. 4 - 5.

18 A. Gaberle, op. cit., s. 25 oraz 41.

19 Internetowa wersja encyklopedii PWN. Wpis dostępny na stronie internetowej pod adresem: http://encyklopedia.pwn.pl/haslo.php?id=3914686.

20 Tak T. Hanausek, Kryminalistyka, Zakamycze 2000, s. 44 - cytuję za A. Lach, Dowody elektroniczne..., op. cit., s. 18.

21 M. Mazur, Cybernetyczna teoria układów samodzielnych, 1966, s. 37.

22 Internetowy słownik języka polskiego PWN. Wpis dostępny na stronie internetowej pod adresem: http://sjp.pwn.pl/slownik/2466189/informacja.

być przetwarzane umysłowo lub maszynowo[23]. W informatyce, przez dane rozumie się także zbiory liczb i tekstów o różnych formach[24], które na najniższym poziomie technicznym reprezentowane są wyłącznie w postaci dwuwartościowej (binarnej), jako ciągi zer i jedynek. W pewnym uproszczeniu, można powiedzieć, że dane, po poddaniu ich odpowiednim przetworzeniom, stanowią materiał do budowy informacji. Pojęciem „danych informatycznych" posługuje się w szczególności polski Kodeks karny, definiując wybrane rodzaje czynów zabronionych. Na gruncie Kodeksu, wskazane wyrażenie wprowadzone zostało do przepisów art. 165 § 1 pkt 4, art. 268a, art. 269, art. 269a oraz art. 287. Wszystkie z wymienionych jednostek redakcyjnych odnoszą się do popełniania przestępstw przy zastosowaniu szeroko rozumianych systemów teleinformatycznych (cyberprzestępstw).

Co istotne, obok pojęcia „danych", w języku nie tylko informatycznym, ale także prawnym, funkcjonuje również wyrażenie „dane komputerowe", które w obecnym stanie prawnym posiada swoją, wiążąca dla Polski, definicję legalną. Definicja ta, przyjęta pierwotnie na gruncie postanowień Konwencji o cyberprzestępczości (w art. 1 lit. b)[25], a następnie inkorporowana do prawa Unii Europejskiej - do przepisów Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. (również w art. 1 lit. b)[26] oraz późniejszej Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne (art. 2 lit b)[27], przyjęła odpowiednio następujące brzmienie:

w Decyzji:

> „dane komputerowe" oznaczają wszelkie przedstawienie faktów, informacji lub pojęć w formie odpowiedniej do przetwarzania w systemie informatycznym, włącznie z programem odpowiednim do spowodowania wykonania funkcji przez system"[28],

---

23 Na podstawie: A. Gadomski: *Global TOGA Meta-Theory*, 1989. Przytaczam za internetową encyklopedią wiedzy, dostępną pod adresem: http://pl.wikipedia.org/wiki/Dane.

24 Na podstawie: G. Wilson: Przetwarzanie danych dla programistów, 2006. Przytaczam za internetową encyklopedią wiedzy, dostępną pod adresem: http://pl.wikipedia.org/wiki/Dane.

25 Tytuł oryginalny: *Convention on Cybercrime*, CETS Nr: 185. Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm. Oficjalny przekład polski dostępny w Dzienniku Urzędowym z 2015 r., poz. 728.

26 Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW. Pełny tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:PL:PDF.

27 Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW. Pełny tekst dyrektywy dostępny na stronie internetowej pod adresem: http://bip.ms.gov.pl/Data/Files/_public/bip/prawo_eu/ue2/dyrektywa-2013_40_ue-o-cyberprzestepczosci.pdf.

28 Definicja w języku polskim pochodzi z oficjalnego tłumaczenia przywołanej Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne. W Konwencji o cyberprzestępczości, definicja przyjęła w oryginale brzmienie: *„"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program*

oraz w Dyrektywie:

> „dane komputerowe" oznaczają przedstawienie faktów, informacji lub pojęć w formie nadającej się do przetwarzania w systemie informatycznym, włącznie z programem umożliwiającym wykonanie funkcji przez system informatyczny"[29].

Uzupełniająco, w Raporcie Wyjaśniającym do Konwencji o cyberprzestępczości[30], na temat przytoczonej definicji można przeczytać również, że:

> „Definicja danych komputerowych została oparta na definicji pochodzącej ze standardu ISO. Definicja ta zawiera zwrot „w formie odpowiedniej do przetwarzania". Zwrot ten oznacza, że dane zapisane są w takiej formie, która umożliwia ich bezpośrednie przetworzenie przez system komputerowy. W celu jednoznacznego określenia, że dane, o których mowa w niniejszej Konwencji, rozumiane są jako dane występujące w elektronicznej lub innej bezpośrednio przetwarzalnej formie, wprowadzone zostało właśnie pojęcie „danych komputerowych". Dane komputerowe, które są przetwarzane automatycznie mogą stać się celem jednego z przestępstw opisanych w niniejszej Konwencji, jak również przedmiotem zastosowania jednego ze zdefiniowanych w Konwencji środków dochodzeniowo-śledczych."[31].

Pomocniczo, Konwencja o cyberprzestępczości wprowadza także dwie szczególne kategorie danych komputerowych. Są nimi:

1) dane stanowiące treść (tzw. *content data*, w Polskim przekładzie Konwencji użyto zwrotu „dane dotyczące treści"); oraz,
2) dane dotyczące ruchu sieciowego (tzw. *traffic data*).

Choć pojęcia te nie zostały zdefiniowane w Konwencji, ich znaczenie można z powodzeniem zrekonstruować na podstawie kontekstu, w którym występują w Konwencji, a także w oparciu o powszechnie przyjęte znaczenie analizowanych określeń. I tak, dane stanowiące treść to innymi słowy dane budujące zawartość przekazów, wiadomości e-mail, czy też dokumentów

---

suitable to cause a computer system to perform a function".

29 Definicja w języku polskim pochodzi z oficjalnego tłumaczenia przywołanej Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne.

30 *Explanatory Report*, pełen tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

31 Raport Wyjaśniający, pkt 25. W oryginale: *„25. The definition of computer data builds upon the ISO-definition of data. This definition contains the terms "suitable for processing". This means that data is put in such a form that it can be directly processed by the computer system. In order to make clear that data in this Convention has to be understood as data in electronic or other directly processable form, the notion " computer data" is introduced. Computer data that is automatically processed may be the target of one of the criminal offences defined in this Convention as well as the object of the application of one of the investigative measures defined by this Convention.*". Tłumaczenie własne.

zapisanych w formie plików. Są to dane, których przechwytywanie poddawane jest szczególnym rygorom, jako istotnie naruszające prawa i wolności człowieka i obywatela. Dane dotyczące ruchu sieciowego, to z kolei dane wskazujące ogólnie na fakt zestawiania połączeń sieciowych, odwiedzania określonych stron WWW, czy też korzystania z określonych usług sieciowych. Jak słusznie zauważa się w doktrynie, praktyczna granica pomiędzy oboma tymi rodzajami danych coraz częściej ulega zatarciu, z uwagi na techniczne aspekty identyfikacji danych w sieci. Przykładowo, otworzenie odsyłacza pozwalającego wyłącznie na pobranie określonych treści nielegalnych, jest jednocześnie informacją o samym ruchu sieciowym (fakt nawiązania połączenia pomiędzy węzłami sieciowymi), jak również o podjęciu próby uzyskania danej treści (informacja o tym, co stanowiło przedmiot transmisji danych). Ostatecznie, Konwencja posługuje się jeszcze określeniem „informacje odnoszące się do abonenta", które to informacje - nie stanowiące ani danych budujących treść, ani też danych o ruchu sieciowym, mogą być przetwarzane w formie danych komputerowych. Zgodnie z przepisem art. 18 ust. 3 Konwencji, informacje te służą do identyfikacji abonenta oraz ogólnie - świadczonych na jego rzecz usług sieciowych.

Powyższa charakterystyka danych pozwala stwierdzić, że na gruncie prawnym nieuzasadnione byłoby stawianie znaku równości pomiędzy kategoriami „danych" oraz „informacji". O ile bowiem dane (stanowiące pojęcie prawnie zdefiniowane) to - w najprostszym ujęciu, dowolnie duża porcja bitów, a więc ciąg zer i jedynek[32], jak również zbudowany z takich danych program komputerowy, o tyle walor informacji, może w systemach teleinformatycznych zostać przypisany jedynie takim danym, które składają się na pełną *wiadomość*, komunikowalną użytkownikowi systemu - człowiekowi. Ostatecznie, warto też podkreślić, że zarówno na gruncie przepisów Konwencji o cyberprzestępczości, jak również przywołanej Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, „systemy komputerowe" (pojęcie stosowane w Konwencji), czy też „systemy informatyczne" (pojęcie stosowane w Decyzji Ramowej), służą właśnie do przetwarzania danych, nie zaś informacji[33]. Analogiczne rozwiązanie funkcjonuje również w obowiązującym, krajowym stanie prawnym. Zgodnie z przepisem art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[34], systemem teleinformatycznym jest:

---

[32] Takie porcje danych w systemie binarnym określane są też mianem BLOB'ów - określenie to stanowi skrót od nazwy *Binary Large Object*. Więcej na ten temat na stronach internetowych dostępnych pod adresami: http://www.techterms.com/definition/blob, czy też http://en.wikipedia.org/wiki/Binary_large_object.

[33] Por. art. 1 lit. a Konwencji o cyberprzestępczości oraz analogiczny art. 1 lit. a Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW.

[34] Dz. U. Nr 144, poz. 1244, z późn. zm.

„zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie **danych** poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnej urządzenia końcowego w rozumieniu ustawy z dnia 17 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)".

Innymi słowy, automatycznemu przetwarzaniu poddawane są dane, stanowiące materiał zrozumiały dla komputerów (oraz innych urządzeń elektronicznych), nie zaś informacje - będące komunikatami czytelnymi dla człowieka.

Na marginesie poczynić należy jeszcze jedną uwagę wobec zaprezentowanej terminologii przyjętej na gruncie Konwencji o cyberprzestępczości oraz przywołanej powyżej Decyzji Ramowej. Odniesienie zdefiniowanych w tych aktach „danych" do „komputerów" („dane komputerowe"), wprowadza zupełnie niepotrzebne zawężenie pojęcia „danych" wyłącznie do tych, które przetwarzane są przez komputery - a już nie np. przez nowoczesne telefony komórkowe. Takie definiowanie danych uznać należy w obecnym świecie za błąd jakościowy, odnoszący dane jedynie do wybranej kategorii urządzeń przetwarzających dane.

Podsumowując wybrane definicje pojęć „informacji" oraz „danych", sformułować można następujące wnioski:

1) pojęcia „danych" oraz „informacji" nie są tożsame;
2) pojęcie „informacji" ma charakter pierwotny, a zatem nie poddaje się jednoznacznej definicji przy użyciu innych określeń;
3) pojęcie „danych" ma charakter wtórny i w obszarze funkcjonowania systemów teleinformatycznych oznacza dowolnej długości ciąg znaków poddających się automatycznemu przetwarzaniu - dane tym samym nie muszą składać się w czytelną dla człowieka informację. Np. informacja poddana procesowi szyfrowania[35] zapisana jest w pamięci komputera w postaci danych, jednak do czasu jej dekryptażu nie stanowi informacji zrozumiałej dla człowieka;
4) pojęcie „informacji" nabiera nieco innego znaczenia w kontekście poznania ludzkiego oraz *przetwarzania automatycznego* - w tym komputerowego. Dla ludzi informacją jest pewnego rodzaju wyobrażenie o określonym stanie faktycznym, dla maszyn - mierzalna różnica wyodrębnionych stanów;
5) w języku potocznym, funkcjonuje - nieuzasadnione z punktu widzenia technicznego, jak również prawnego, utożsamianie informacji oraz danych.

[35] Jak zwraca uwagę B. Fischer - szyfrowanie jest prawnie dopuszczalne i stanowi istotne zagrożenie dla osiągania celów procesu karnego, tak w: B. Fischer, op. cit, s. 113.

Mając za sobą przybliżenie znaczenia pojęć „informacja" oraz „dane", możliwe jest w następnej kolejności podjęcie próby udzielenia odpowiedzi na następujące pytanie: jaki wpływ na zakres przedmiotowy pojęcia „dowodu elektronicznego" ma zastosowanie w jego różnych definicjach przyjęcia, jako *genus* - bądź to danych (komputerowych), bądź też informacji?

Co zostało podkreślone na końcu poprzedniego fragmentu rozdziału, zgodnie z obowiązującym stanem prawnym - zarówno międzynarodowym, jak również krajowym, zadaniem szeroko rozumianych systemów teleinformatycznych (także informatycznych, komputerowych) jest automatyczne przetwarzanie danych. Innymi słowy, cyfrowa materia poddawana obróbce przez całą infrastrukturę cyberprzestrzeni - w tym też pojedyncze komputery jej użytkowników, przyjmuje formę właśnie danych. Część z tych danych składa się na informacje - a więc komunikaty wyrażone w formie (w szczególności w języku) zrozumiałej dla ludzi. Pozostała część danych nie przybiera natomiast waloru tak identyfikowanej informacji, pozostając „zrozumiałą", czy wręcz „postrzegalną" wyłącznie dla świata maszyn. Przykładem pierwszej kategorii danych mogą być dane tworzące pliki tekstowe, w szczególności dokumenty, strony internetowe zawierające określone treści, czy wreszcie zawartość programów komputerowych, jak również ich kod źródłowy - zawierający informacje o sposobie działania danego programu. Jako przykłady danych nie tworzących informacji wskazać można natomiast dane wykorzystywane *wewnętrznie* do samej organizacji pracy systemów teleinformatycznych (np. wymieniane w ramach wydawania przez procesor określonych poleceń kierowanych do pamięci komputera), dane przechowywane w systemach podręcznie celem przyspieszenia pracy, czy też niektóre dane związane z organizacją ruchu sieciowego, jak choćby dane służące do nawiązania połączenia pomiędzy systemami. Informacjami nie należy nazywać także danych niekompletnych, niepozwalających użytkownikowi na odczytanie określonego komunikatu (otworzenie dokumentu, odtworzenie nagrania multimedialnego, itd.), jak również danych zaszyfrowanych, na co wskazywano wcześniej. Informacją nie są także już skompilowane programy komputerowe występujące w formie niezrozumiałego dla ludzi kodu maszynowego. Stąd właśnie, przytoczone wyżej definicje „danych komputerowych" wyraźnie obejmowały także oprogramowanie komputerowe, wykluczając je tym samym ze zbioru desygnatów pojęcia „informacja". W prostej konkluzji, można stwierdzić, że w odniesieniu do cyberprzestrzeni, z punktu widzenia zakresu potencjalnego materiału dowodowego, kategoria informacji stanowi zbiór znacznie zawężony w stosunku do zbioru danych komputerowych.

Z uwagi na powyższe, definiowanie dowodu elektronicznego poprzez odnoszenie go

do informacji uznaję za błędne z następujących powodów:

- systemy teleinformatyczne nie przetwarzają informacji zaś dane - definiowanie dowodu elektronicznego z zastosowaniem pojęcia informacji stanowi zatem wynik swoistego pomieszania pojęć odnoszących się do z jednej strony do sfery poznania ludzkiego oraz z drugiej - sfery zautomatyzowanego funkcjonowania szeroko rozumianych urządzeń elektronicznych,
- nie wszystkie dane tworzą informację, a zatem ograniczanie zakresu przedmiotowego dowodu elektronicznego do informacji wyklucza możliwość traktowania, jako taki dowód szerokiego katalogu danych,
- z punktu widzenia procesowego, ewentualne zabezpieczenie informacji wymaga szczegółowego wskazania przedmiotu tak zdefiniowanej czynności. W przypadku zabezpieczania danych, możliwe jest zabezpieczenie np. danych całego dysku twardego, bez uprzedniego ustalania, czy zapisane na nim dane w ogóle składają się na jakiekolwiek informacje,
- z uwagi na rosnące zastosowanie technik kryptograficznych, dane zaszyfrowane nie powinny być wyłączane spod kategorii dowodu elektronicznego. Dane takie, nie stanowiąc informacji czytelnej dla człowieka, mogą być uznawane za dowód elektronicznych wyłącznie w przypadku jego definiowania z zastosowaniem odniesienia do kategorii danych komputerowych,

Na marginesie warto też przypomnieć, że stosowanie w polskiej ustawie kategorii informacji w odniesieniu np. do samego definiowania cyberprzestępstw, stanowi naruszenie zasad implementacji do porządku krajowego przepisów międzynarodowych, definiujących poszczególne cyberprzestępstwa, jako czyny kierowane przeciwko nie informacjom, zaś danym komputerowym. Niespójność ta powoduje dodatkowe trudności w ramach analizy problematyki wykorzystywania dowodów elektronicznych, o czym Autor pisze w dalszej części pracy.

§2. Pojęcia używane w odniesieniu do śladów cyberprzestępczości

Obok wyrażenia „dowód elektroniczny”, w językach tak prawniczym, jak i prawnym, funkcjonują także inne pojęcia mające określać szeroko rozumiane ślady popełnionych cyberprzestępstw. I choć wiele z nich pochodzi z doktryny amerykańskiej, bogatej w rozważania na temat przestępczości nowoczesnych technologii, określenia istotne z punktu widzenia prowadzonej w tym miejscu analizy można znaleźć także w opracowaniach

kontynentalnych. Przybliżenie wybranej grupy takich określeń uważam za zasadne przynajmniej z dwóch powodów - wskazanie dodatkowych pojęć pozwala na przedstawienie pełniejszego obrazu stosowanej na świecie siatki pojęciowej; oraz - umożliwia zwrócenie uwagi na cechy charakterystyczne poszczególnych wyrażeń, pogłębiając zrozumienie szeroko rozumianej problematyki dowodów cyberprzestępczości.

Pierwszym z pojęć, chyba najczęściej konkurującym z „dowodem elektronicznym", jest zwrot „dowód cyfrowy" (*digital evidence*)[36]. O ile samo sformułowanie „dowód elektroniczny" nakazuje odnosić swoje znaczenie do wszelkich materiałów występujących w formie elektronicznej - a więc takiej, która w najprostszym ujęciu opiera się na ruchu impulsów elektrycznych w układzie zawierającym elementy aktywne[37], o tyle zwrot „dowód cyfrowy" zawęża tak zakreślony zbiór desygnatów wyłącznie do tych *dowodów elektronicznych*, które funkcjonują w postaci cyfrowej (w opozycji do postaci analogowej) - w praktyce zaś, głównie binarnej (zero-jedynkowej). Dla przykładu, zabezpieczona kopia pliku komputerowego mieści się w obydwu wskazanych kategoriach, stanowiąc zarówno dowód cyfrowy (plik posiada zapis binarny), jak i dowód elektroniczny (zapis impulsów). Z drugiej strony, np. nagrania z kamer analogowych, pomimo posiadania formy elektronicznej (np. zapis na specjalnej taśmie), nie mogą być zaliczane do materiałów cyfrowych, jako że ich zapis przyjmuje postać właśnie analogową, nie zaś cyfrową. Warto też dodać, że Międzynarodowa Organizacja do spraw Dowodów Komputerowych (*International Organisation on Computer Evidence - IOCE*[38]) zdefiniowała „dowód cyfrowy", jako:

> „informację przechowywaną lub transmitowaną w formie binarnej, która może mieć znaczenie w postępowaniu sądowym"[39]

- niejako przesądzając, że w obecnym czasie pojęcie „cyfrowy" należy utożsamiać z zapisem binarnym (zero-jedynkowym).

Drugim, również często stosowanym pojęciem, jest określenie „dowód komputerowy" (*computer evidence*)[40], wskazujące nie tyle na formę potencjalnych dowodów (elektroniczna -

---

[36] Zob. np.: E. Case, op. cit., czy też A. J. Marcella, F. Guillossou w: *Cyber Forensics: From Data to Digital Evidence,* Wydawnictwo John Wiley & Sons, New Jersey 2012.

[37] Na podstawie wpisu pochodzącego z otwartej encyklopedii sieciowej, zamieszczonego na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/Elektronika.

[38] Organizacja funkcjonowała w ramach prac Grupy G8, faktycznie rozwiązanej w 2014 r. Więcej o organizacji na stronie internetowej dostępnej pod adresem: www.ioce.org.

[39] Definicję przywołują w piśmiennictwie m. in. K. J. Pawelec, op. cit., s. 25 oraz A. Lach w: Dowody elektroniczne..., op. cit., s. 30, a także w: Dowody cyfrowe..., op. cit., s 1. Tekst opracowania dostępny jest na stronie internetowej pod adresem: http://www.bibliotekacyfrowa.pl/Content/24720 /Dowody_cyfrowe_w_postepowan.pdf

[40] Zob. np. C. Brown, *Computer Evidence: Collection and Preservation,* Charles River Media 2009, czy też M. Dahl, *Computer Evidence*, Capstone 2004. Także: E. Wilding, *Computer Evidence: A Forensic*

nie elektroniczna, cyfrowa - analogowa), co powiązanie dowodu z określonym rodzajem urządzenia źródłowego, jakim jest komputer. Z konieczności technicznej, ponieważ komputer jest urządzeniem elektronicznym oraz cyfrowym, „dowód komputerowy" musi być zatem także „dowodem elektronicznym" oraz „dowodem cyfrowym". Niemniej, trudno za tak rozumiany dowód komputerowy uznać np. materiał zabezpieczony w telefonie komórkowym. Telefon - choćby najnowocześniejszy, trudno jest nazwać komputerem, choć funkcjonalność zaawansowanych *smartfonów* zbliża zakres ich zastosowania do możliwości jeszcze niedawno zarezerwowanych wyłącznie dla komputerów. Tym samym, z punktu widzenia semantycznego, na tle opozycji pojęć „dowód komputerowy" - „dowód elektroniczny", powstaje wątpliwość, czy pliki komputerowe po zgraniu do pamięci telefonu mogą być zabezpieczane w tymże telefonie, jako *dowody komputerowe*? Trzymając się strony literalnej, dowód z telefonu, nie jest dowodem z komputera. Z drugiej jednak strony, wydaje się niezasadnym aby o rodzaju dowodu przesądzał wyłącznie sam typ urządzenia, z którego dowód ten został uzyskany. Proponując rozwiązanie przedstawionego problemu, być może za dowód komputerowy należałoby uznawać każdy materiał, który z uwagi na swoją budowę może być przetwarzany na komputerze.

Trzecim pojęciem odnoszącym się do oznaczania śladów cyberprzestępstw, o nieco już historycznym zabarwieniu, jest natomiast sformułowanie „dowód wytworzony na komputerze" (*computer-generated evidence*)[41]. Istotą tak określonego materiału, jest fakt jego wygenerowania wewnątrz pamięci komputera, co pozwala podkreślić pierwotny brak materialnego substratu takiego dowodu. Dowodem bowiem nie jest w tym wypadku pamięć komputera (czyli innymi słowy nośnik), w której znajdują się impulsy elektryczne, lecz pewna treść - wyrażona oryginalnie jako dane, która to treść jest w pamięci komputera przetwarzana. Treść taka może zostać następnie poddana procesowi *de-cyfryzacji*, w drodze choćby zwykłego wydruku - czy to wydruku określonej porcji danych, czy też informacji wytworzonych na komputerze (np. wydruk logu określającego szczegóły ruchu sieciowego na określonym węźle). Dowodem wytworzonym na komputerze jest zatem każdy materiał, do którego stworzenia zastosowany został komputer, bez względu na formę, w jakiej materiał ten znajduje się w chwili jego analizy.

Co zasługuje na odrębne podkreślenie, wielokrotnie przywoływana w niniejszej pracy Konwencja o cyberprzestępczości również nie posługuje się pojęciem „dowodu elektronicznego", zastępując je jednak określeniem bliskoznacznym - „dowodu w formie

---

Investigations Handbook, Londyn 1997 - wskazuję za: A. Lach, Dowody elektroniczne op. cit., s. 29.

[41] Zob. np. G. Joseph, *Modern Visual Evidence*, American Lawyer Media, Nowy Jork 1984.

elektronicznej" (*evidence in electronic form*)[42]. Pojęcie to nie zostało niestety w żaden sposób zdefiniowane na gruncie Konwencji, czy choćby przybliżone w załączonym do Konwencji Raporcie Wyjaśniającym[43]. Zastosowane odwołanie do formy elektronicznej pozwala wyraźnie zaznaczyć, że dowodem, o którym stanowi Konwencja, może być nie tylko materiał, który oryginalnie wytworzony został w formie elektronicznej, ale także materiał, który formę taką uzyskał w sposób wtórny - np. poprzez zeskanowanie dokumentu oraz wprowadzeniu go do systemu. Niemniej, pojęcie „dowodu elektronicznego" w żadnym razie nie wyklucza z kręgu swoich desygnatów także i takich materiałów, które formę elektroniczną nabyły wtórnie, co w istocie nadaje obydwu terminom charakter synonimiczny. Co również warto w tym miejscu zauważyć, w przywołanym Raporcie Wyjaśniającym do Konwencji, w jego pkt 243, wyrażenia „*evidence in electronic form*" oraz „*electronic evidence*" użyte są wręcz zamiennie, choć to drugie określenie występuje w całym dokumencie jedynie raz. Sama Konwencja posługuje się natomiast konsekwentnie pojęciem „dowodu w formie elektronicznej". Na marginesie - nieco starszy dokument Rady Europy, pod której auspicjami prowadzone były prace nad Konwencją o cyberprzestępczości, noszący miano Zalecenia Nr R (95) 13 Komitetu Ministrów Rady Europy w sprawie „Problemów karnoprocesowych związanych z technologią przetwarzania informacji" z 11 września 1995 r., posługiwał się w swoim tekście zwrotem „*electronic evidence*"[44]. Przyjęcie jednolitej siatki terminologicznej wydaje się w takiej sytuacji elementem niezbędnym dla wytworzenia przyszłych, wspólnych regulacji procesowych, które miałyby regulować kwestie transgranicznego (w szczególności w wymiarze globalnym) pozyskiwania oraz wykorzystywania zdobytych w ten sposób dowodów elektronicznych.

Podsumowując dotychczasowe rozważania, należy zauważyć, że pomimo występowania wielu różnych pojęć określających ślady popełnienia cyberprzestępstw, to właśnie określenie „dowód elektroniczny" stosowane jest najczęściej w doktrynie prawnej. Jego zakres pozwala objąć szerokie spektrum materiałów, inkorporując desygnaty pojęć: dowody elektroniczne-analogowe (np. nagrania o charakterze analogowym), dowody cyfrowe

[42] Określenie to użyte jest w przepisach Konwencji pięciokrotnie: w art. 14 ust. 2 lit. c, art. 23, art. 25 ust. 1, art. 35 ust. 1 oraz art. 46 ust. 1 lit. b. Pełny tekst konwencji dostępny jest na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[43] *Explanatory Report*, pełen tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[44] Tytuł oryginalny: „*Problems of Criminal Procedural Law Connected with Information Technology. Recommendation No. R (95) 13 adopted by the Committee of ministers of the Council of Europe on 11 September 1995 and explanatory memorandum*", Council of Europe Publishing, 1996. Tekst dokumentu dostępny jest na stronie internetowej pod adresem: „http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp".

(przyjmujące postać binarną), jak również dowody przetwarzane przy użyciu komputera oraz wszelkich innych urządzeń elektronicznych. Dowodem elektronicznym może być jednocześnie zarówno materiał zapisany lokalnie na pojedynczym komputerze, jak również materiał przetwarzany w cyberprzestrzeni, w szczególności zaś transmitowany poprzez sieć.

§3. Informatyczne nośniki danych, jako nośniki dowodów elektronicznych

Jak zostało zauważone powyżej, praca systemów teleinformatycznych opiera się na przetwarzaniu danych. Przetwarzanie to nie mogłoby jednak odbywać się bez zastosowania w systemach odpowiednich rodzajów pamięci elektronicznych, umożliwiających chwilowe lub też trwałe przechowywanie wszelkich efektów operacji wykonywanych na danych. W zależności od wymaganego zastosowania pamięci, do zapisu danych wykorzystywana jest w szczególności pamięć podręczna procesora (tzw. *cache*[45]), pamięć operacyjna systemu (tzw. RAM[46]), pamięć zainstalowana w układach graficznych (np. w technologii GDDR) oraz pamięć trwałych nośników danych - magnetycznych dysków twardych[47], pamięci półprzewodnikowych[48] (jak np. dyski SSD, czy też pamięci przenośne w technologii *flash*), czy wreszcie wszelkiego rodzaju nośniki optyczne (płyty CD, DVD oraz BD[49])[50]. O ile pierwsze trzy kategorie pamięci należą do tzw. pamięci ulotnych (ich zapis ma charakter tymczasowy oraz znika wraz z wyłączeniem maszyny z prądu), pozostałe wymienione nośniki danych oferują pamięć nieulotną, której wyczyszczenie następuje - co do zasady, z woli użytkownika systemu. Z uwagi na budowę oraz zasady działania, pamięci nieulotne charakteryzuje jednak czasowa możliwość odczytu nawet uprzednio usuniętych danych. Nietrwale wyczyszczone nośniki mogą zatem zawierać „na swojej powierzchni" także wcześniej przetwarzane na nich dane, stanowiąc tym samym potencjalne źródło materiału dowodowego[51].

---

[45] Więcej na temat pamięci podręcznych na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Pami%C4%99%C4%87_podr%C4%99czna.

[46] Skrót od angielskich wyrazów *Random Access Memory*. Więcej na temat pamięci operacyjnej na stronie internetowej pod adresem: https://pl.wikipedia.org/wiki/RAM.

[47] Więcej na temat budowy oraz zapisu danych na dysku twardym na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Dysk_twardy

[48] Więcej na temat pamięci półprzewodnikowych na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Pami%C4%99%C4%87_p%C3%B3%C5%82przewodnikowa

[49] Więcej o zapisie optycznych nośników danych na stronach internetowych dostępnych pod adresami: http://pl.wikipedia.org/wiki/Dyski_CD, http://pl.wikipedia.org/wiki/DVD oraz http://pl.wikipedia.org/wiki/Blu-ray, a także http://pl.wikipedia.org/wiki/Pit oraz http://pl.wikipedia .org/wiki/Land_(dyski_optyczne).

[50] Por. B. Fischer, op. cit., s. 114 i nast.

[51] Z prowadzonych badań wynika, że znakomita większość dysków twardych nie jest czyszczona (z ang. *wipe*) przed ich odsprzedażą, czy też utylizacją, zagrażając w szczególności tajemnicom handlowym nieostrożnych firm. Więcej na ten temat na stronach internetowych dostępnych pod adresami:

Nieco inna sytuacja charakteryzuje natomiast dane pozostające w trakcie transmisji poprzez sieci teleinformatyczne. W trakcie bowiem swojej podróży pomiędzy kolejnymi węzłami cyberprzestrzeni, przekazywane dane nie przyjmują na najniższym, fizycznym poziomie, postaci zapisu na nośniku, zaś postać czystych impulsów lub fal elektromagnetycznych, transmitowanych w ramach zestawionego połączenia sieciowego[52]. Swoistym „nośnikiem" danych stają się w tej sytuacji łącza sieciowe, które mogą przybierać postać infrastruktury kablowej (przewody miedziane lub też kable światłowodowe) lub też infrastruktury radiowej. Należy jednak podkreślić, że łącza sieciowe nie zapewniają przechowywania danych, stanowiąc jedynie „autostradę" dla danych[53], łączącą kolejne węzły sieci - czyli serwery, zaopatrzone - tak, jak komputery osobiste, w różne rodzaje pamięci elektronicznych, umożliwiających szeroko rozumiane przetwarzanie danych (jak np. dalsze przekazywanie pobranych oraz skolejkowanych danych, czy też zwrotne wysyłanie danych żądanych przez użytkownika strony internetowej). W pewnym uproszczeniu, zaś nieco bardziej obrazowo, można powiedzieć, że bez pamięci elektronicznych zainstalowanych w systemach nadawczym oraz odbiorczym, poszczególne pakiety danych transmitowane poprzez sieci niemiałyby gdzie się „gromadzić" w treści, które budują, jako całość. W przypadku zaś przechwytywania danych pomiędzy łączami (przy ewentualnym wpięciu w kabel łączący węzły lub też podsłuchu łączności radiowej), pozyskiwany ruch sieciowy również musi być gromadzony w postaci zapisu danych na określonym nośniku danych.

Ponieważ zatem wszystkie dane przetwarzane są ostatecznie w systemach przy wykorzystaniu różnego rodzaju nośników pamięci elektronicznych, można powiedzieć, że nośniki danych reprezentują swoisty substrat materialny danych, zawierając na sobie elektromagnetyczny (w przypadku pamięci półprzewodnikowych lub magnetycznych) lub fizyczny (w przypadku pamięci optycznych - to jest płyt, które wypalane są laserem) zapis danych. Oczywiście nie należy z tego powodu utożsamiać samego nośnika z pojęciem „dowodu elektronicznego", bowiem dowodem jest zawsze określona treść zapisana na tym nośniku, nie zaś sam nośnik[54]. Niemniej, ponieważ zapis danych pozostaje nierozerwalnie złączony z określonym nośnikiem (to jest zapisu danych nie można „wyjąć" z nośnika, oddzielając te dwa elementy), wszelkie gromadzone dane, zawsze będą znajdować się na

---

http://www.esecurityplanet.com/windows-security/how-to-securely-delete-data-from-hard-drives.html, oraz http://readwrite.com/2008/11/16/how_to_permanently_delete_data.

[52] Tak: J. Błachut, Dokument jako przedmiot ochrony prawnokarnej, Lex, Warszawa 2011, s. 44 - 45.

[53] W tym sensie łącza sieciowe stanowią jedynie specyficzne środowisko transmisji danych, dla których nie-fizycznym nośnikiem w sensie logicznym stają się same impulsy elektromagnetyczne podróżujące w przewodach. Tak: J. Błachut, op. cit., s. 41.

[54] *Ibidem*, s. 41.

nośnikach danych.

W prawie polskim nośniki służące do przetwarzania danych zdefiniowane zostały w przepisach dwóch aktów normatywnych:

1) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[55]; oraz
2) rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego[56] - wydanego na podstawie art. ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[57].

Zgodnie z art. 3 pkt 1 przywołanej ustawy, pod pojęciem „informatycznych nośników danych" (bowiem taką nazwę otrzymały wskazane powyżej pamięci w prawie krajowym), należy rozumieć:

> „materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej".

Komentując powyższą definicję, należy podkreślić jej następujące cechy:

– informatycznym nośnikiem danych nazwane zostały „materiały lub urządzenia" zapewniające możliwość realizacji określonej w dalszej części definicji funkcjonalności. Ponieważ jednak żadne ze wskazanych pojęć - to jest ani „materiał", ani „urządzenie", nie posiadają swoich definicji legalnych, można zauważyć, że przyjęty *genus* definicji, w istocie nie precyzuje, czym są nośniki danych. W rozumieniu potocznym, materiałem nazwać można bowiem w zasadzie każdy przedmiot, skąd też alternatywne dopisanie do definicji „urządzenia" wydaje się być zabiegiem nadmiarowym, mającym ewentualnie wskazać na konieczność traktowania, jako nośników, także urządzeń z wbudowaną pamięcią - a zatem nie tylko pamięci pozwalających się fizycznie odseparować od np. reszty systemu (jak choćby dyski twarde, które można wyjąć z komputera),
– wyliczona w przepisie funkcjonalność nośników - zapisywanie, przechowywanie i odczytywanie, wydaje się być sformułowana zbyt wąsko oraz niekonsekwentnie. Zapisywanie oraz przechowywanie to czynności w istocie tożsame, tak więc opisujące jedną funkcjonalność. Odczytywanie zaś, nie wyczerpuje z kolei wszystkich

[55] Dz. U. Nr 64, poz. 565, z późn. zm. Pełny tekst aktu dostępny jest na stronie internetowej pod adresem: http://isap.sejm.gov.pl/DetailsServlet?id=WDU20050640565.

[56] Dz. U. Nr 159, poz. 948. Pełny tekst aktu dostępny jest na stronie internetowej pod adresem: http://isip.sejm.gov.pl/DetailsServlet?id=WDU20111590948.

[57] Dz. U. Nr 182, poz. 1228. Pełny tekst aktu dostępny jest na stronie internetowej pod adresem: http://isip.sejm.gov.pl/DetailsServlet?id=WDU20101821228.

pozostałych zastosowań nośników. O ile bowiem nośniki same w sobie nie przetwarzają danych (w systemach czyni to przede wszystkim procesor - CPU), ich udział w przetwarzaniu danych jest niezbędny, bowiem wszelkie operacje na danych wykonywane są w przestrzeni pamięci systemu. Ponadto, przyjęta w definicji konstrukcja semantyczna - stanowiąca, że nośnikiem jest także „urządzenie", uzasadnia twierdzenie, że nośniki mogą być wykorzystywane do szeroko rozumianego przetwarzania danych, nie zaś tylko ich „gromadzenia" oraz „wydawania" (np. laptop z wbudowanym na stałe dyskiem SSD z pewnością nie służy jedynie do wskazanych czynności),

– ostatecznie, należy podkreślić, że w samym końcu definicji, jej zakres przedmiotowy został ograniczony wyłącznie do nośników „danych w postaci cyfrowej". Oznacza to, że „informatycznymi nośnikami danych" nie jest możliwe nazywania nośników informacji zapisanych w postaci analogowej, zaś wyłącznie cyfrowej - co w praktyce oznacza zawężenie analizowanego pojęcia do nośników umożliwiających zapis danych w postaci binarnej (zero-jedynkowej).

Drugi z przywołanych aktów normatywnych, to jest rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, którego zakres przedmiotowy - co warto zaznaczyć, dotyczy wyłącznie sfery przetwarzania informacji niejawnych, również posługuje się zwrotem „informatyczny nośnik danych", wprowadzając do przyjętej w ustawie definicji wyłącznie jedną zmianę o charakterze redakcyjnym. I tak, zgodnie z przepisem § 2 pkt 4 rozporządzenia, informatycznym nośnikiem danych jest:

„materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej".

W stosunku do definicji pochodzącej z ustawy, projektodawca rozporządzenia usunął z przygotowanej definicji zwrot „lub urządzenie", który to zabieg miał na celu zapewnienie zgodności definicji z przepisami ustawy o ochronie informacji niejawnych, zawierającej delegację ustawową do wydania przywołanego rozporządzenia. Zgodnie bowiem z art. 2 pkt 4 ustawy o ochronie informacji niejawnych, materiałem jest „dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia". Tym samym, na gruncie tejże ustawy, pojęcie „urządzenia" mieści się już w zakresie desygnatów pojęcia „materiał".

Pojęcie „informatycznego nośnika danych" wykorzystane zostało także w Kodeksie

karnym, gdzie pojawia się jednak wyłącznie dwukrotnie w przepisach penalizujących dwa rodzaje cyberprzestępstw (są to: art. 268 § 2 - niszczenie zapisu istotnej informacji, oraz art. 269 § 2 - niszczenie danych o szczególnym znaczeniu dla obronności kraju oraz jego bezpieczeństwa). Kodeks karny nie zawiera jednak własnej definicji wskazanego wyżej pojęcia.

Odwoływanie się do jakiegokolwiek rodzaju nośników danych nie zostało natomiast wprowadzone do postanowień Konwencji o cyberprzestępczości[58], jak również Decyzji Ramowej Unii Europejskiej w sprawie ataków na systemy informatyczne[59] oraz Dyrektywy Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne[60].

§4. Istota dowodów elektronicznych - ich cechy szczególne oraz wybrane klasyfikacje

Mając za podstawę do dalszych rozważań poczynione wyżej uwagi o charakterze ogólnym - na gruncie których zakreślony został katalog pojęć stosowanych w odniesieniu do śladów cyberprzestępstw wraz z ich definicjami, a także przybliżona została problematyka informatycznych nośników danych - niniejsza część rozdziału poświęcona została cechom szczególnym dowodów elektronicznych, pozwalającym odróżnić tak nazwaną kategorię dowodów od dowodów *tradycyjnych*, występujących poza systemami teleinformatycznymi. Przedstawienie cech szczególnych dowodów elektronicznych zostało także oparte na prezentacji wybranych klasyfikacje śladów cyberprzestępstw.

Odwołując się do charakterystyki dowodów elektronicznych przedstawionej przez A. Lacha[61], jako najistotniejszy atrybut dowodów elektronicznych należy wskazać ich szczególną formę, pozbawioną typowych atrybutów fizycznych[62]. Dowodem elektronicznym nie jest zatem określone urządzenie elektroniczne (np. komputer), zainstalowany w tym urządzeniu informatyczny nośnik danych (np. dysk twardy), czy wreszcie fizyczny lub

---

58 Tytuł oryginalny: *Convention on Cybercrime*, CETS Nr: 185. Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

59 Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, Nr 2005/222/WSiSW. Pełny tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:PL:PDF.

60 Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW. Pełny tekst dyrektywy dostępny na stronie internetowej pod adresem: http://bip.ms.gov.pl/Data/Files/_public/bip/prawo_eu/ue2/dyrektywa-2013_40_ue-o-cyberprzestepczosci.pdf.

61 A. Lach, Dowody elektroniczne w procesie karnym, Towarzystwo Naukowe Organizacji i Kierownictwa, Dom Organizatora, Toruń 2004, s. 32.

62 M. Kliś, Przestępczość w Internecie. Zagadnienia podstawowe, Czasopismo Prawa Karnego i Nauk Penalnych, Wydawnictwo Polska Akademia Umiejętności, Kraków 2000, opracowanie dostępne na stronie internetowej pod adresem: http://prawo.vagla.pl/node/905.

magnetyczny zapis danych, zlokalizowany na nośniku - lecz same dane, które ten zapis reprezentuje[63]. Co było wskazywane wyżej, oczywiście żadne dane nie mogą istnieć bez jakiegokolwiek nośnika, który pozwoliłby na ich - choćby krótkotrwałe, utrwalenie, jednak w dalszym ciągu z pojęciem dowodu elektronicznego nie mogą być utożsamiane dowolne substraty fizyczne danych. Twierdzenie to nabiera szczególnego znaczenia w kontekście możliwości bezstratnego powielania danych, które to powielanie może być dokonywane zarówno lokalnie - to jest w sytuacji, gdy osoba wykonującą kopię danych posiada fizyczny dostęp do określonego nośnika danych, jak również w drodze transmisji danych poprzez węzły cyberprzestrzeni lub też sieci lokalnej (np. z pozycji administratora systemu). Poruszana forma dowodów elektronicznych pozwala na przeprowadzenie ich podziału wedle wielu kryteriów klasyfikacyjnych, spośród których wybrane zostały te, które w ocenie Autora niniejszej pracy pozwalają na przeprowadzenie najpełniejszej charakterystyki oraz prezentacji istotnych cech dowodów elektronicznych.

Z uwagi na fakt, iż dane budujące dowody elektroniczne mogą składać się na materiały różnego rodzaju - biorąc pod uwagę szczególną formę elektroniczną dowodów, można je podzielić na następujące kategorie ze względu na reprezentowane treści[64]:

1) dowody zawierające czytelny dla człowieka tekst (w szczególności dokumenty elektroniczne, a więc materiały sporządzone w formie pisemnej oraz utrwalone w postaci elektronicznej), zapisane w szczególności w plikach o rozszerzeniach .doc, .pdf, czy też .txt;
2) dowody zawierające obrazy - dane składające się na zapis zdjęć, filmów, nagrań z kamer itd., niezależnie od rodzaju (analogowy - cyfrowy) oraz formatu zapisu (np. w plikach o rozszerzeniach .jpg., .gif, .avi, .mpg, czy też formatach specjalistycznych, wysoce skompresowanych oraz zabezpieczonych, jak np. formaty służące do rejestracji odcisków palców, zdjęcia biometryczne, itd.);
3) dowody zawierające zapis dźwięku - dane tworzące nagrania audialne, podobnie jak w przypadku materiałów graficznych, zapisane bądź to jako dane cyfrowe, bądź też analogowe, niezależnie od formatu zapisu (w szczególności rozszerzenia plików .wav,

[63] Tak np.: A. Adamski, Prawo karne komputerowe, CH Beck, Warszawa 2000, s. 199, czy też A.Lach, Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia teoretyczne i praktyczne, e-biuletyn CBKE 2/2004, Wrocław 2004, s 1 - 2. Tekst opracowania dostępny jest na stronie internetowej pod adresem: http://www.bibliotekacyfrowa.pl/Content/24720/Dowody_cyfrowe_w_postepowan.pdf.

[64] Przedstawiona klasyfikacja została oparta na podziale zaprezentowanym przez A. Lacha w: Dowody elektroniczne w procesie karnym, Towarzystwo Naukowe Organizacji i Kierownictwa, Dom Organizatora, Toruń 2004, s. 37, oraz uzupełniona o spostrzeżenia własne.

.mp3 oraz formaty specjalistyczne, stosowane np. w nagraniach uzyskiwanych w toku stosowania kontroli operacyjnej);

4) dowody zawierające dane o pracy systemu - tzw. logi lub też zapisy audytowe (z ang. *audit trails*), pozwalające na odtworzenie historii pracy systemu oraz np. rekonstrukcje *modus operandi* sprawcy ataku cybernetycznego. Szczególnym rodzajem danych o pracy systemu są tzw. pliki *cookies* (w stosowanym coraz częściej tłumaczeniu „ciasteczka") czyli pliki przechowujące lokalnie na komputerze użytkownika informacje o jego aktywności w ramach różnych usług sieciowych - np. informacje o fakcie zalogowania z zastosowaniem określonego *loginu*; oraz,
5) dowody zawierające dane, które tworzą kod maszynowy oprogramowania, a więc skompilowane pliki programów, wykonywalne wyłącznie przez przystosowane do tego urządzenia (np. komputer PC ze stosownym systemem operacyjnym[65]). Dane takie są zupełnie nieczytelne dla człowieka, *vide* wcześniejsze uwagi o charakterze technicznym poczynione na gruncie rozdziału III pracy.

W zależności od utrwalonych w dowodzie treści, pierwsze trzy spośród wymienionych wyżej kategorii dowodów elektronicznych, mogą być kwalifikowane w rozumieniu procesowym zarówno jako dokumenty[66], jak i właściwe dowody rzeczowe[67]. Przykładowo, dowody zawierające czytelny dla człowieka tekst mogą stanowić nie tylko zapis ludzkiej myśli (np. oświadczenie sporządzone w postaci elektronicznej), ale mogą być także materiałami generowanymi automatycznie - to jest z pominięciem człowieka, które winny być wówczas traktowane jako dowody rzeczowe (np. potwierdzenie wykonania określonej operacji w systemie). Jak bowiem podkreśla się w doktrynie prawa karnego procesowego, na gruncie procedury karnej za dokument uważa się przede wszystkim utrwalony zapis ludzkiej myśli, stanowiący formę wypowiedzi autora[68]. Tym samym, o kwalifikacji dowodu elektronicznego, jako dokumentu (elektronicznego) winna decydować jego treść, nie zaś wyłącznie forma. Analogicznie, zapis dźwięku, czy obrazu, które co do zasady kojarzone są z dowodami

---

[65] Należy zauważyć, iż programy komputerowe nie zapewniając tzw. interoperacyjności pomiędzy różnymi systemami operacyjnymi. Przykładowo, programy systemu Windows nie działają w środowiskach Unix, jak np. w systemie Linux w dowolnej dystrybucji.

[66] Zgodnie ze sposobem rozumienia przywołanych pojęć wyrażonym w kanonie piśmiennictwa, np.: A. Gaberle, op. cit., s. 41 i nast., s. 45 i nast., S. Waltoś, op. cit., s. 349, 346 - 347 oraz 353 i nast., T. Grzegorczyk, J. Tylman, op. cit., Warszawa 2011, s. 463 oraz s. 470 i nast., T. Grzegorczyk, Dowody w procesie karnym, Wydawnictwo Prawnicze, Warszawa 1998, s. 4 i nast, s. 12 i nast., oraz s. 100 i nast., czy też J. Błachut, op. cit., s. 41 i nast., s. 119 - 120, oraz s. 126 lub K. J. Pawelec, op. cit., s. 24 i nast.

[67] Na dopuszczalność obydwu kwalifikacji zwraca uwagę A. Lach w: Dowody elektroniczne..., op. cit., s. 32.

[68] Tak np.: T. Nowak, Dowód z dokumentu w polski procesie karnym, Poznań 1994, s. 23 - 25, czy też T. Grzegorczyk, J. Tylman, op. cit., s. 483. Przytaczam za A. Lach, Dowody elektroniczne..., op. cit., s. 43.

rzeczowymi, mogą również zawierać przekazy intelektualne, charakteryzując się cechami właściwymi dla dokumentu. Jako dokumenty nie powinny być natomiast kwalifikowane dowody zawierające dane o pracy systemu (logi), jak również dane tworzące skompilowany kod oprogramowania (np. nielegalna kopia programu). Powyższe stanowisko nie jest jednak jednoznaczne wśród przedstawicieli doktryny prawnej, gdzie pojawiają się zdania odrębne np. odmawiające zapisom obrazu możliwości kwalifikacji, jako dokumentu[69], przy jednoczesnym - zupełnie niekonsekwentnym, uznawaniu za dokument wybranych nagrań dźwiękowych. Sytuacja ta potwierdza jedynie konieczność dostosowania funkcjonujących narzędzi prawnych do nowych wymagań stawianych konstrukcji procesu karnego na tle zagadnień związanych ze zwalczaniem przestępczości cyberprzestrzeni. Ostatecznie warto też podkreślić, że materiały dźwiękowe oraz graficzne, często występują w postaci połączonej, jako nagrania audio-wizualne. Ocena, czy taki materiał stanowi dowód rzeczowy, czy dokument, musi być dokonywana z zastosowaniem ogólnych zasad prawnych, odwołujących się do analizy podstawowych elementów materiału dowodowego.

Dotykając kwestii funkcjonowania tzw. dokumentów elektronicznych, za niezbędne dla prowadzenia dalszej analizy problematyki pozyskiwania elektronicznego materiału dowodowego, należy uznać także bliższe przedstawienie aktualnego stanu prawnego, regulującego czym w istocie jest „dokument elektroniczny". Pojęcie to posiada bowiem nie tylko swoją konotację prawną, ale przede wszystkim - ustawową definicję legalną. Zgodnie z przepisem art. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[70] - której to ustawy przepisy należy traktować, jako centralne w systemie krajowego prawa informatycznego, za „dokument elektroniczny" należy uznawać:

> „stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych.".

Co wynika wprost z przytoczonej definicji, dokumentem elektronicznym są zatem dane - a więc nie informacje, które zostały zapisane w postaci elektronicznej na informatycznym nośniku danych. Tak ujętym dokumentem elektronicznym mogą być zarówno materiały występujące w formie cyfrowej (binarnej)[71], jak również analogowej. Jednocześnie – w świetle przyjętej definicji, dokumentem elektronicznym nie muszą być wcale materiały przybierające postać pisemną, jak również materiały w ogóle czytelne dla człowieka.

[69] Tak np. T. Nowak, op. cit., s. 32.
[70] Dz. U. Nr 64, poz. 565.
[71] *Vide* analizowana w pierwszej części rozdziału definicja IOCE pojęcia „dowód cyfrowy" oraz poczynione tam uwagi.

Odwołanie się w definicji do danych powoduje bowiem objęcie jej zakresem przedmiotowym wszelkich danych, niezależnie od tego czy reprezentują tekst, nagrania audiowizualne, czy też np. kod programu komputerowego. Osobliwą formą dokumentu elektronicznego stanowią również bazy danych, których zawartość może łączyć w sobie wszystkie wymienione rodzaje treści, scalając je w jedną całość o spójnej, ściśle określonej strukturze wewnętrznej. To ostatnie pojęcie należy bowiem - w ocenie Autora niniejszej dysertacji - rozumieć, jako wymóg aby dane budujące dokument elektroniczny, posiadały ustaloną formę, pozwalającą na ich odczytanie (choćby automatyczne) oraz dalsze przetwarzanie. Za tak rozumiane struktury należy zatem uznawać np. przyjętą strukturę plików, jak choćby tych o rozszerzeniach .doc, .pdf, czy też .gif, co oznacza odniesienie „wewnętrznej struktury danych" do poziomu technicznego budowy danych, nie zaś ich poziomu znaczeniowego. Tak pojmowana wewnętrzna struktura w żadnej mierze nie musi odnosić się wyłącznie do sposobu rozmieszczenia danych na dokumencie tekstowym zapisanym w postaci elektronicznej (np. lokalizacja pola „miejsce sporządzenia dokumenty, data sporządzenia dokumentu"), zaś określa samą strukturę danych, według której dane te przetwarzane są przez stosowne urządzenie informatyczne. W praktyce, zdecydowaną większość dokumentów cyfrowych będzie stanowić pliki komputerowe - a więc materiały cyfrowe. Dla kwalifikacji dokumentu elektronicznego nie jest jednocześnie istotne, czy dokument ten został oryginalnie wytworzony w systemie, czy też został do systemu wprowadzony, np. w drodze zeskanowania lub innej formy digitalizacji.

Obok powyższej definicji legalnej dokumentów elektronicznych - zawartej w akcie rangi ustawowej, co więcej stanowiącym akt centralny w systemie przepisów odnoszących się do informatyzacji kraju, szczególną definicję pojęcia „dokumentów elektronicznych", stworzoną na potrzeby regulacji odnoszących się do ochrony informacji niejawnych, wprowadza także rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów niejawnych i umieszczania na nich klauzul tajności[72]. Zgodnie z przepisem § 2 pkt 3 wskazanego aktu, ilekroć w rozporządzeniu wydanym do ustawy o ochronie informacji niejawnych, jest mowa o „dokumencie elektronicznym" (stawianym w opozycji do „dokumentu nieelektronicznego"), należy przez to rozumieć:

> „dokument utrwalony na informatycznym nośniku danych lub przetwarzany w systemie teleinformatycznym, o ile ze względu na organizację obiegu informacji niejawnych

[72] Dz. U. Nr 288, poz. 1692.

podlega rejestracji".

Przytoczona definicja wprowadza w stosunku do definicji ustawowej dwie istotne różnice w pojmowaniu tego, czym jest dokument elektroniczny:

- po pierwsze, o ile definicja ustawowa określa, jako swój *genus* - dane, o tyle definicja zawarta w rozporządzeniu odwołuje się do kategorii „dokumentu". W ujęciu ściśle językowym, rozwiązanie to może być uznawane za błąd definicyjny *idem per idem* (dokument elektroniczny to dokument). Zważywszy jednak na sposób rozumienia pojęcia „dokument" w znaczeniu przyjętym na gruncie przepisów o ochronie informacji niejawnych, dokumentami są te materiały niejawne, których treść wyrażona jest w formie pisemnej, a zatem tak charakteryzowanym dokumentem elektronicznym, są te *pisma*, które zostały zapisane w wersji elektronicznej. Jak podkreśla się w literaturze, analizowana w tym miejscu definicja pojęcia „dokument" wyrażona na gruncie ustawy o ochronie informacji niejawnych obejmuje swoim zakresem tak egzemplarze dokumentu wytworzone oryginalnie, jak również wszystkie jego późniejsze kopie[73],
- po drugie, definicja zawarta w rozporządzeniu odnosi się nie tylko do tych dokumentów, które zostały zapisane na informatycznym nośniku danych - jak czyniła to definicja ustawowa, lecz również do dokumentów przetwarzanych w systemie teleinformatycznym. Wprowadzone rozszerzenie należy w ocenie piszącego te słowa rozumieć, jako wskazujące iż dokumentem elektronicznym jest nie tylko materiał już zapisany (wytworzony), ale również materiał przetwarzany w pamięci ulotnej urządzenia (np. w pamięci RAM w przypadku komputera klasy PC). Rozszerzenie to należy uznawać za istotne z punktu widzenia zasad ochrony informacji niejawnych, które to informacje muszą podlegać szczególnym rygorom także w trakcie ich wytwarzania, gdy nie posiadają jeszcze swojego trwałego zapisu na nośniku danych.

Wykluczenie z definicji pochodzącej z rozporządzenia odniesienia do określonej struktury danych, można tłumaczyć obecnością przepisów określających szczegółowo sposób oznaczania materiałów niejawnych, narzucający ściśle reglamentowaną strukturę dokumentów zawierających chronione informacje.

Choć pojęcie dokumentu elektronicznego nie występuje na gruncie przepisów Kodeksu karnego ani też Kodeksu postępowania karnego, pierwsza z wymienionych ustaw kodeksowych, definiując pojęcie „dokumentu", odnosi je również do dokumentów zapisanych

[73] Tak np. J. Błachut, op. cit., s. 122.

na nośnikach, przez co należy rozumieć również informatyczne nośniki danych. Zgodnie z przepisem art. 115 § 14 Kodeksu karnego:

> „Dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym związane jest określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne."

Tym samym, w świetle przytoczonej kodeksowej definicji dokumentu, te spośród dokumentów elektronicznych - w rozumieniu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, z którymi związane jest określone prawo lub stanowią dowód prawa, stosunku prawnego lub też prawnie relewantnej okoliczności - będą stanowić obok dokumentu elektronicznego także dokument w rozumieniu przepisów Kodeksu karnego. Pozostałe dokumenty elektroniczne - np. ukazujące lub potwierdzające poprawny stan pracy systemu teleinformatycznego, nie będą mogły uzyskać takiej kwalifikacji. Niemniej, logi systemowe stanowiące zapis przebiegu (a w konsekwencji dowód) popełnienia ataku cybernetycznego winny być zawsze kwalifikowane, jako dokumenty, a to z racji na zawartą w nich treść, potwierdzającą okoliczność o znaczeniu prawnym - to jest popełnienie stypizowanego w ustawie czynu zabronionego. Subsydiarnie, wskazane dokumenty będą musiały być traktowane, jako szczególne dowody rzeczowe, pozostając w kręgu desygnatów szerszego zakresowo pojęcia „dowód elektroniczny"[74]. Zarysowaną niekompatybilność przepisów rangi ustawowej należy traktować jako wyraz niedbałości tworzenia rozwiązań systemowych w zakresie szeroko pojętego prawa informatycznego[75].

Wracając do analizy kwalifikacji dowodów elektronicznych, z uwagi na ich szczególną formę, dowody te można również podzielić stosując kryterium powstania zapisu, na następujące kategorie:

1) dowody elektroniczne *pierwotne*; oraz,
2) dowody tzw. zdigitalizowane[76].

Jako dowody elektroniczne pierwotne określić należy te materiały, które oryginalnie zostały wytworzone w formie elektronicznej - a więc w szczególności dane zapisane w plikach komputerowych, czy też różnego rodzaju nagrania audio-wizualne. Dowodami zdigitalizowanymi są zaś te materiały, które formę elektroniczną uzyskały wtórnie, to jest np. w drodze zeskanowania podpisanego odręcznie dokumentu (aktualnie coraz częściej

---

74 Kwestie te porusza A. Lach w: Dowody cyfrowe..., op. cit., s .7.

75 Na konieczność standaryzacji technicznych aspektów postępowania z dowodami cyfrowymi uwagę zwraca A. Lach w: Dowody cyfrowe..., op. cit., s .7.

76 Pojęciem tym posługuje się A. Lach, przeciwstawiając mu jednak kategorię dowodów „cyfrowych *sensu stricto*". Tak w: A. Lach, Dowody elektroniczne..., op. cit., s. 37 oraz 57 - 61.

prowadzi się proces tzw. dematerializacji dokumentów, w szczególności w odniesieniu do różnego rodzaju zasobów archiwalnych, bibliotecznych, itd.). Poszukując zwrotu legalnego, który mógłby oznaczać ów sygnalizowany w piśmiennictwie proces digitalizacji, warto odwołać się do zdefiniowanego prawnie terminu „odwzorowanie cyfrowe", pojawiającego się na gruncie przepisów przywoływanego wyżej rozporządzenia Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów niejawnych i umieszczania na nich klauzul tajności[77]. Choć wskazane rozporządzenie wydane zostało do ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych - co oznacza, iż jego zakres przedmiotowy obejmuje wyłącznie tę kategorię informacji, istotnym *novum* wskazanego aktu normatywnego jest próba uregulowania na jego gruncie kwestii właśnie zmiany formy dokumentów z nieelektronicznej (innymi słowy papierowej) na elektroniczną. Zgodnie z przepisem § 2 pkt 6 rozporządzenia przez pojęcie „odwzorowanie cyfrowe" należy rozumieć:

> „przekształcenie dokumentu nieelektronicznego w dokument elektroniczny, dokonywane w szczególności przez jego zeskanowanie".

Jednocześnie też, na gruncie rozporządzenia, poprzez kopiowanie dokumentów, należy rozumieć:

> „w szczególności wykonywanie odpisu, wypisu, wyciągu, wydruku, odwzorowania cyfrowego lub nagrania".

Analizując sytuację dowodów elektronicznych wytworzonych wtórnie, należy zaznaczyć, iż materiały odwzorowywane cyfrowo stanowią w istocie kopię oryginalnego materiału. Z punktu widzenia procesowego zatem, zgodnie z zasadą bezpośredniego dostępu do materiału dowodowego, o ile istnieje możliwość uzyskania dostępu do materiału oryginalnego, przeprowadzenie takiej czynności dowodowej wydaje się niezbędne. Elektroniczna kopia dokumentu może natomiast zastąpić jego oryginał, w przypadku utraty lub zniszczenia jego postaci papierowej. Co oczywiste, zeskanowany podpis odręczny, nie nabywa w żadnej mierze cech podpisu elektronicznego, nie spełniając ustawowych przesłanek wyrażonych na gruncie ustawy z dnia 18 września 2001 r. o podpisie elektronicznym[78].

Ostatecznie, szczególna forma dowodów elektronicznych pozwala także na przeprowadzenie jeszcze jednego ich podziału, z uwzględnieniem kryterium źródła, z którego uzyskany został określony materiał dowodowy[79]. Tak określone kryterium umożliwia

---

[77] Dz. U. Nr 288, poz. 1692.
[78] Tekst jednolity ustawy został opublikowany w Dz. U. z 2013 r., poz. 262.
[79] Przedstawiony podział został oryginalnie zaproponowany przez prof. A. Adamskiego w: Prawo karne...,

wyodrębnienie dwóch, następujących kategorii dowodów elektronicznych[80]:

1) dowody elektroniczne przechwycone w czasie transmisji, zebrane w ramach kontroli operacyjnej lub podsłuchu procesowego;
2) dowody elektroniczne tworzone przez dane zapisane lokalnie na informatycznych nośnikach danych.

Co było przedmiotem poszerzonej analizy prowadzonej na gruncie rozdziału III niniejszej pracy, wszelkie dane występujące w obszarze cyberprzestrzeni wpierw wytwarzane są lokalnie - wewnątrz dających się wydzielić układów systemów teleinformatycznych (może to być pojedynczy komputer, ale też domowa sieć lokalna, czy sieć korporacyjna), by następnie odbywać cyber-podróże, skacząc po kolejnych węzłach pośredniczących w ruchu sieciowym transmitowanym od nadawcy do adresata.

Przywołane w tym miejscu kryterium podziału dowodów elektronicznych zwraca zatem uwagę na „miejsce", z którego określona porcja danych - stanowiących dowód, została pobrana. Stosując uproszczoną analogię do nieco bardziej konwencjonalnych środków przekazu, można powiedzieć, że pozyskiwanie danych przetwarzanych lokalnie wewnątrz systemów przypomina fizyczne uzyskanie dostępu do mieszkania oraz „przeszukanie" np. jeszcze niewysłanej, ale już przygotowanej do wysłania korespondencji. Z kolei pozyskiwanie danych transmitowanych przez sieci należy przyrównać do przechwytywania korespondencji już nadanej, tzn. takiej, która zgodnie z jego życzeniem opuściła siedzibę nadawcy oraz znajduje się aktualnie w dyspozycji urzędu pocztowego, czy tez kuriera, zapewniającego dostarczenie przesyłki. Obydwie te czynności mogą wiązać się zarówno z odczytem treści, które zostały zapisane w przesyłkach lub też ograniczać się wyłącznie do pozyskania informacji o adresacie listu. Wracając na grunt przekazu danych, należy zauważyć, że ponieważ wszelkie dane transmitowane poprzez węzły cyberprzestrzeni zostają wytworzone lokalnie (to jest na określonym systemie teleinformatycznym), a jednocześnie wysyłanie danych polega na przekazywaniu nie tyle „określonego egzemplarza danych", co danych identycznych (w istocie ich kopii) - wszelkie dane, które mogą zostać przechwycone w ruchu, mogą też zostać „złapane" wewnątrz systemu, z którego zostały nadane. Za przykład obrazujący wskazaną zależność może posłużyć krótki opis funkcjonowania korespondencji wysyłanej drogą elektroniczną, stanowiącej istotne źródło dla pozyskiwania dowodów elektronicznych:

op. cit., s. 192.

[80] Kategorie te zaznacza także A. Lach w: Dowody cyfrowe..., op. cit., s .2.

- tzw. poczta e-mail może być wysyłana zarówno bezpośrednio z komputera nadawcy (w przypadku, gdy korzysta on z tzw. klienta poczty, np. programu Microsoft Outlook, czy też Mozilla Thunderbird), jak również z jego komputera za pośrednictwem aplikacji sieciowej udostępnionej przez dostawcę usług pocztowych (np. sieciowa aplikacja pocztowa Google o nazwie Gmail). Niezależnie od przyjętej metody, każda wiadomość pocztowa wytwarzana jest najpierw na komputerze nadawcy, by następnie zostać przesłaną dalej, do adresata. Różnica pomiędzy wskazanymi wyżej sposobami sporządzania poczty (klient lokalny lub aplikacja sieciowa) polega na określeniu miejsca, gdzie zostanie przechowana trwała kopia wiadomości - w przypadku lokalnych klientów poczty, wiadomości zostają zapisane bezpośrednio na dysku twardym komputera nadawcy, skąd są wysyłane do adresata za pośrednictwem właściwego węzła wybranej usługi pocztowej (dane węzła wprowadza się do programu pocztowego w trakcie konfiguracji konta). W przypadku korzystania z aplikacji sieciowych - wiadomość sporządzana jest na komputerze nadawcy, przechowywana krótkotrwale w ulotnej pamięci jego komputera, a następnie wysyłana na serwer pocztowy, tam trwale zapisywana i ostatecznie przekazywana już przez serwer dalej do adresata. Po zamknięciu strony internetowej z aplikacją pocztową (choćby przywołanej poczty gmail.com), wiadomość nie występuje fizycznie w pamięci komputera nadawcy,
- mając powyższe na uwadze, z punktu widzenia technicznego, wiadomości poczty elektronicznej mogą być przechwytywane zarówno wewnątrz komputera nadawcy (jako trwałe kopie wiadomości wysłanych, czy też obraz wiadomości przetwarzanych chwilowo w ulotnej pamięci komputera - do momentu ich wysłania na serwer), jak również już „w drodze" poprzez kolejne węzły pośredniczące w ruchu sieciowym. Dodatkowo - w przypadku gdy poczta przechowywana jest na serwerze nadawczym lub odbiorczym (np. jako kopia bezpieczeństwa, czy też dla wygody - by zapewnić dostępność do wszelkiej posiadanej korespondencji z dowolnego komputera podłączone do sieci), wiadomości mogą być przechwytywane także bezpośrednio z pamięci tychże serwerów, analogicznie do przechwytywania poczty nagranej lokalnie na komputerze nadawcy. Innymi słowy - dane przetwarzane lokalnie, to nie tylko dane zapisane bezpośrednio na komputerze nadawcy, ale dane zapisane trwale wewnątrz dowolnego systemu, niepodlegające wysyłaniu, lecz (czasowo) zarchiwizowane,

- przygotowane do wysłania oraz już wysłane wiadomości pocztowe zawierają oznaczenie nie tylko nadawcy przesyłki, ale także jej adresata. Należy mieć jednak na uwadze, iż adres docelowy poczty elektronicznej w żadnym razie nie przesądza, kto pocztę tę odbierze, ani z którego komputera - czy też z jakiego adresu IP identyfikującego określone, fizyczne zakończenie sieci, wykona tę czynność. W istocie, adresy nadawczy oraz docelowy poczty e-mail najczęściej identyfikują wyłącznie podmioty obsługujące serwery poczty elektronicznej, wskazując tym samym na administratora poczty, z którym należy kontaktować się dla ustalenia dalszych danych precyzujących fizyczną lokalizację serwera pocztowego, na który trafi dana wiadomość (np. adres e-mail: b.morawski@wp.pl zawiera informację, iż podmiotem obsługującym konto pocztowe jest podmiot Wirtualna Polska, będący właścicielem zawartej w adresie poczty elektronicznej domeny wp.pl),
- w każdym z przybliżonych przypadków, dane budujące określoną wiadomość pocztową są co do zasady takie same, a więc źródło pozyskania danych nie ma znaczenia w kontekście oceny, czy to treści, czy też formy przechwyconych danych. Nie można jednak zapomnieć, iż każda porcja danych może zostać uszkodzona lub umyślnie zmodyfikowana w ramach popełnienia jednego z cyberprzestępstw przeciwko dostępności lub integralności danych. Wystąpienie takiego czynu może w konsekwencji spowodować np. różnicę pomiędzy treścią poczty zapisanej w komputerze nadawcy oraz obsługującym go serwerze pocztowym, a w efekcie - różnicę pomiędzy treścią kopii wiadomości, a treścią wiadomości rzeczywiście wysłanej,
- ostatecznie, warto też podkreślić, że poczta elektroniczna - tak jak każda inna forma przekazu elektronicznego, może zawierać nie tylko treści pisane, ale również nagrania audio-wizualne, czy też tzw. przekazy „na żywo" - np. rozmowy głosowe, czy wideo konferencje (jak w przypadku technologii Skype).

Tak jak w przypadku przechwytywania komunikatów przekazywanych z wykorzystaniem innych mediów transmisyjnych, tak też dane dot. poczty elektronicznej mogą być pozyskiwane w zakresie pełnym - to jest wraz z treścią wiadomości, jak również ograniczonym wyłącznie do danych opisujących sam ruch sieciowy (analogicznie do opozycji: kontrola operacyjna treści rozmów - pozyskiwanie tzw. danych bilingowych). Kwestie oceny prawnej pozyskiwania danych poruszane są w następnej części pracy, która poświęcona została zagadnieniom transpozycji „konwencjonalnych" czynności procesowych

do obszaru cyberprzestrzeni.

Obok wyżej wskazanego atrybutu dowodów elektronicznych, jakim jest ich szczególna forma, dowody te można również dzielić stosując odwołania do innych, nieco bardziej konwencjonalnych sposobów podziału materiału dowodowego. W szczególności, warto w tym miejscu zwrócić uwagę na dwie klasyfikacje uzupełniające podział dowodów elektronicznych zbudowany w oparciu o ich szczególną formę, zaproponowany przez A. Lacha[81]. I tak, dowody elektroniczne można podzielić także:

1. ze względu na typ dowodu, na:
    1) właściwe dowody rzeczowe; oraz,
    2) dokumenty[82].
2. ze względu na wartość dowodu, na:
    1) dowody samoistne; oraz;
    2) dowody niesamoistne.

Przytoczone kryteria pozwalają na przybliżenie dwóch dodatkowych cech charakteryzujących istotne właściwości dowodów elektronicznych:

- po pierwsze, dowody elektroniczne, stanowiące co do zasady dowody rzeczowe (jako zapis określonych treści, zawarty na informatycznym nośniku danych lub transmitowany poprzez sieci oraz utrwalony w wyniku przechwycenia) mogą przybierać postać szeroko rozumianych dokumentów, ale także wszelkiego rodzaju materiałów (danych) komputerowych, w żadnym razie nieczytelnych dla człowieka pozbawionego dostępu do komputera. Materiały należące do drugiej z wymienionych kategorii należy pojmować oraz oceniać w sposób analogiczny do materiałów stanowiących np. narzędzia zbrodni lub wszelkiego rodzaju kryminalistyczne ślady jej popełnienia. W szczególności należy wskazać tu na kod tzw. oprogramowania złośliwego będącego narzędziem przeprowadzenia ataku cybernetycznego oraz logi systemowe, stanowiące zapis historii pracy systemu - w tym wszelkich czynności, które nie były planowane przez administratorów systemu. Kwestia stosunku dowodów elektronicznych do *elektronicznych narzędzi zbrodni* analizowana jest w kolejnym punkcie rozdziału,
- po drugie zaś, podział dowodów elektronicznych na dowody samoistne oraz niesamoistne pozwala w sposób istotny uzupełnić wcześniejsze rozważania na temat

[81] A. Lach, Dowody elektroniczne..., op. cit., s. 38
[82] Uzupełniająco, A. Lach, Dowody cyfrowe..., op. cit., s. 2 i nast. Autor podkreśla iż „w polskim procesie karnym dokumenty są często uznawane za szczególną formę dowodów rzeczowych".

podziału przestępczości komputerowej na przestępczość zamykającą się w całości w cyberprzestrzeni (przede wszystkim ataki cybernetyczne, gdzie zarówno naruszane dobro prawne, jego przedmiot, jak i *modus operandi* działania sprawcy występują w samej cyberprzestrzeni) oraz tę, w której działalność w cyberprzestrzeni stanowi jeden z elementów określonego procederu przestępnego (np. wykorzystanie sieci, wyłącznie jako medium do wyłudzenia danych, które będą następnie wykorzystywane dalej do popełnienia np. kradzieży środków finansowych). Dowodami samoistnymi będą zatem te dowody, które odnoszą się do cyberprzestępczości *sensu stricte*, zaś niesamoistnymi - dowody odnoszące się do tych czynów, w których cyberprzestrzeń stanowi jedynie medium dla popełnienia przestępstwa. W świetle powyższego stwierdzenia, należy jednoznacznie nie zgodzić się ze stwierdzeniem, iż „zazwyczaj dowody elektroniczne będą miały charakter dowodów przypadkowych, powstających poza postępowaniem karnym i nie dla jego celów”[83]. W odniesieniu do cyberprzestępczości zdefiniowanej w rozdziale II pracy, dowody elektroniczne stanowią bowiem główny materiał opisujący przebieg danego ataku cybernetycznego, który z racji na swoją nie-fizyczną, lecz *cyberprzestrzenną* specyfikę, pozostawia równie elektroniczne ślady przestępstwa.

§5. Analiza stosunku zachodzącego pomiędzy dowodem cyberprzestępstwa, a faktycznym narzędziem jego popełnienia

Co zostało opisane szerzej na gruncie rozdziału III niniejszej pracy, na najniższym poziomie technicznym, wszelkie procesy przetwarzania danych informatycznych - w tym także ruch sieciowy, polegają w istocie na przekazywaniu niezliczonych ilości słabych impulsów elektrycznych, których dwuwartościowa budowa symbolizuje bity informacji. Ponieważ wszelkie zatem dane informatyczne - czy to zapisane na nośnikach, przetwarzane przez procesor, czy wreszcie przechowywane chwilowo w ulotnej pamięci operacyjnej komputera - zachowują homogeniczną budowę, dane stanowiące *dowód* (lub też zapis) popełnienia cyberprzestępstwa, nie różnią się formą od danych, które stanowiły *narzędzie* jego popełnienia. Każde cyberprzestępstwo popełnione zostaje bowiem poprzez wywołanie odpowiedniej reakcji atakowanego systemu, powodowanej (niczym reakcja alergiczna), wprowadzeniem do tego systemu zestawu odpowiednio przygotowanej paczki danych – w szczególności komend, kodu oprogramowania złośliwego, czy spreparowanych,

[83] A. Lach, Dowody elektroniczne..., op. cit., s. 32.

fałszywych informacji. W konsekwencji, w wielu przypadkach, zestaw danych, które posłużyły za narzędzie do przeprowadzenia cyberataku, będzie również stanowić podstawowy, a czasami wręcz jedyny, dowód popełnienia czynu zabronionego. Zależność zachodzącą pomiędzy narzędziem a dowodem cyberprzestępstwa można zobrazować na następujących przykładach:

- w przypadku ataku *phishingowego* (mającego na celu wyłudzenie m. in. haseł i loginów do usług bankowych), przeprowadzanego poprzez rozsyłanie do ofiar ataku spreparowanych wiadomości poczty elektronicznej, rozesłana wiadomość stanowić będzie zarówno narzędzie zbrodni, jak również dowód usiłowania jej popełnienia. Dane budujące przedmiotową wiadomość będą jednocześnie identyczne w przypadku ich porównania po zabezpieczeniu na komputerze ofiary, która wiadomość odebrała oraz na komputerze atakującego. Inaczej niż w przypadku posłużenia się bronią palną do popełnienia zabójstwa, narzędzie cyberprzestępstwa zostanie wielokrotnie powielone, zapisując swoje kopie w pamięci wielu systemów, w tym także systemów pośredniczących w ruchu sieciowym, który dokonuje się pomiędzy maszynami atakującą oraz atakowaną,
- podobnie, ataki przeprowadzane za pomocą oprogramowania złośliwego polegają najczęściej na wprowadzeniu do atakowanego systemu wykonywalnego kodu, który wykonuje w tle określone działania, z reguły zupełnie nieuświadamiane przez uprawnionego użytkownika systemu. Dowodem popełnienia tak opisanego przestępstwa wprowadzenia kodu złośliwego jest zestaw danych informatycznych budujących opisany kod, wprowadzonych w sposób nieautoryzowany do wnętrza atakowanej maszyny. Ponownie, kod złośliwego oprogramowania stanowi jednocześnie narzędzie oraz dowód popełnienia przestępstwa, powielający się w wielu systemach teleinformatycznych - w szczególności atakującym oraz atakowanym. Transmisja danych nie polega bowiem na wysyłaniu poprzez sieci „tych egzemplarzy" danych, które przetwarzane są lokalnie przez komputer, lecz w istocie ich kopii, to jest danych *idealnie* takich samych,
- z drugiej strony - o ile zadaniem oprogramowania złośliwego jest podsłuchiwanie danych przetwarzanych na zaatakowanym komputerze - czyli ponownie, robienie kopii tych danych oraz wymuszanie na zaatakowanym komputerze ich wysyłania pod określony adres odbiorczy, dowodem takiej działalności przestępnej jest analiza ruchu sieciowego, która pozwala na ustalenie nieautoryzowanego eksportu danych poza system. Ostatecznie, jednoznacznym dowodem nielegalnego pozyskania danych

- czy to zdobytych z pamięci zaatakowanego komputera, czy też przechwyconych w trakcie transmisji danych na jednym z węzłów pośredniczących, jest wreszcie także samo potwierdzenie zapisu nielegalnej kopii danych w pamięci maszyny atakującej lub na informatycznym nośniku danych. W tej sytuacji, narzędzie popełnienia przestępstwa - jakim jest wprowadzony do systemu kod oprogramowania złośliwego, stanowi dowód uzyskania nielegalnego dostępu do systemu (element niezbędny dla wgrania do systemu oprogramowania), zaś dowodem nieautoryzowanego działania kodu jest zapis historii przepływów sieciowych, potwierdzający wykonywanie transmisji danych poza system,

– ataki polegające na wysyłaniu poprzez sieci określonych komend do atakowanych systemów również polegają *de facto* na transmitowaniu danych, tyle, że nieprzybierających formy programu, lecz polecenia, które kierowane jest do oprogramowania już zainstalowanego na komputerze ofiary. Istotna różnica pomiędzy transmisją oprogramowania, a transmisją samych komend, polega jednak na tym, iż w tym drugim przypadku, dane informatyczne budujące komendę najczęściej nie są trwale zapisywane w pamięci komputera. Dane te po wprowadzeniu do określonego programu (np. środowiska bazodanowego) są wykonywane, np. poprzez sprowokowanie systemu do zwrotnego odesłania określonych informacji, zaś sama komenda - jako już zrealizowane polecenie, nie zapisuje się w postaci odrębnego pliku. Wprowadzenie polecenia musi być tej sytuacji rekonstruowane na podstawie analizy ruchu sieciowego wchodzącego oraz następującego w jego konsekwencji ruchu wychodzącego. W ramach historii ruchu zbierane są bowiem wyłącznie informacje opisujące ten ruch (tzw. przepływy sieciowe), zaś nie sama treść ruchu (jego zawartość). Różnicę pomiędzy przepływami a treścią pakietów można przyrównać do różnicy występującej pomiędzy danymi bilingowymi, a treściami przesyłek uzyskiwanymi w ramach stosowania kontroli operacyjnej, czy podsłuchu procesowego. Problematyka źródeł dowodów elektronicznych poddana jest szczegółowej analizie w kolejnej części rozdziału.

Wszystkie wskazane przykłady potwierdzają, iż niezależnie od szczegółowego sposobu działania sprawcy cyberprzestępstwa, dane budujące narzędzie zbrodni (oprogramowanie, komendę, czy spreparowaną do wyłudzania danych stronę WWW lub wiadomość e-mail) stanowią też istotny dowód popełnienia czynu zabronionego. Już samo wprowadzenie w sposób nieautoryzowany danych do komputera ofiary, spełnia bowiem przesłankę

nielegalnego uzyskania dostępu do całości lub części systemu - zagadnieniom charakterystyki oraz kwalifikacji cyberprzestępczości poświęcone zostały rozdziały IV i V niniejszej pracy.

Z punktu widzenia dowodowego, szczególną sytuacją jest traktowanie jako dowodu popełnienia czynu zabronionego samego zapisu historii ruchu sieciowego, potwierdzającego jedynie przekazanie pomiędzy systemami określonej porcji danych. Konieczność taka występuje w przypadkach przesłania komendy oraz zwrotnego wysyłania przez program szpiegujący wykradzionych danych. Historia ruchu sieciowego nie przesądza bowiem treści danych, które zostały przesłane, lecz ukazuje wyłącznie spis połączeń oraz zawiera dane, które opisują te połączenia (np. godzina połączenia, jego kierunek, itd.). Jednoznacznym dowodem wykradzenia danych, jest w tej sytuacji nielegalna kopia danych, występującą po stronie maszyny atakowanej. Z uwagi na poruszane trudności w ustaleniu przedmiotu transmisji danych poprzez sieci, tzw. analiza powłamaniowa, prowadzona po wystąpieniu incydentu komputerowego, nierzadko nie pozwala na jednoznaczne oraz precyzyjne potwierdzenie, które dane zostały skompromitowane w trakcie cyberprzestępstwa oraz dokąd dokładnie zostały przesłane określone ich partie.

§6. Przegląd źródeł dowodów elektronicznych

Scharakteryzowany w powyższy sposób materiał dowodowy występujący w postaci elektronicznej, spotkać można aktualnie w zasadzie w każdym miejscu, w którym tylko odbywa się ludzka aktywność[84]. Z uwagi na postępującą cyfryzację życia, coraz rzadziej obywamy się bez stosowania najróżniejszego rodzaju urządzeń elektronicznych - cyfrowych, które służą nam do szeroko rozumianego przetwarzania informacji, czy też danych (np. zapisywania notatek, budowania arkuszy kalkulacyjnych), wykonywania połączeń głosowych oraz zestawiania telekonferencji, obsługi poczty elektronicznej, dokonywania transakcji z wykorzystaniem kart płatniczych, robienia zdjęć cyfrowych, nagrywania filmów oraz utrwalania nagrań głosowych, czytania tzw. e-książek (*ebook*), czy wreszcie umilania czasu muzyką, filmami, bądź też najróżniejszego rodzaju aplikacjami - w tym grami[85].

Mając na uwadze wcześniejsze uwagi odnoszące się do charakterystyki dowodu elektronicznego, dowodu tego w żadnym wypadku nie należy odnosić wyłącznie do

---

[84] K. J. Pawelec, op. cit., s. 24.

[85] Warto zauważyć, że rynek gier *video* - który do niedawna kojarzony był wyłącznie z rozrywką dla dzieci, aktualnie wytwarza nowe rodzaje usług - jak np. tzw. mikrotransakcje, pozwalające na nabywanie wirtualnych dóbr za całkiem realne pieniądze. Ceny poszczególnych przedmiotów (jak np. broń, zbroje, czy elementy wyposażenia wirtualnego mieszkania) potrafią sięgać nawet tysięcy dolarów rodząc pokusę do ich „cyfrowego podrabiania”, czy też zdobywania w sposób nieuczciwy (np. poprzez zwabienie słabszego gracza w zasadzkę, oraz uśmiercenie kierowanej przez niego postaci celem „ograbienia”).

materiałów zapisanych na komputerze, czy też komputerowych, informatycznych nośnikach danych, takich jak dyski twarde, przenośne pamięci typu *flash* (tzw. *pendrive'y*, przenośne dyski USB), czy też nośniki optyczne (płyty CD, DVD, BD itd.). W związku z powyższym, za zasadne należy uznać przedstawienie możliwie szerokiego przeglądu źródeł dowodowych, z których możliwe jest pozyskiwanie właśnie tak szeroko rozumianych dowodów elektronicznych. Zestawienie takie, pozwoli jednocześnie na płynne przejście do zagadnień następnego rozdziału, to jest kwestii transpozycji konwencjonalnych czynności procesowych - w szczególności zaś czynności z zakresu postępowania dowodowego, do budowanego przez bity informacji świata cyberprzestrzeni.

Ponieważ dane komputerowe - co było już wielokrotnie podkreślane w niniejszej pracy, mogą być przetwarzane zarówno lokalnie, to jest w obrębie jednego urządzenia cyfrowego, jak też w szeroko rozumianej cyberprzestrzeni, a więc w ramach ruchu sieciowego o potencjalnie globalnym zasięgu[86], źródła dowodów elektronicznych można podzielić na dwie robocze kategorie, oddające powyższy rozdział „miejsca", w którym przetwarzane są interesujące dane cyfrowe[87]:

1) źródła odseparowane od cyberprzestrzeni - np. wszelkiego rodzaju pamięci przenośne odpięte od sieci (to jest nie podłączone bezpośrednio do sieci bądź też do urządzeń posiadających czynne połączenie sieciowe);
2) szeroko rozumiane zasoby cyberprzestrzeni - w istocie wszystkie materiały zlokalizowane w dowolnego typu pamięci systemów teleinformatycznych (trwałej, jak i ulotnej) oraz innych urządzeń cyfrowych funkcjonujących w sieci, w szczególności zaś w sieci Internet. Obok poszczególnych systemów stanowiących zakończenia sieci, do tej kategorii źródeł dowodowych zaliczyć należy także wszystkie urządzenia budujące infrastrukturę sieciową (przełączniki, routery, centrale, wszelkie urządzenia komutacyjne itd).

Niezależnie od przypisania określonego źródła dowodowego do pierwszej bądź drugiej kategorii, kategorie te nie wpływają w żadnej mierze na scharakteryzowaną wcześniej istotę dowodów elektronicznych. Co więcej, pojedyncze urządzenia działające w sieci (a więc należące do kategorii drugiej) po ich odpięciu od łącza, czy też na wskutek zablokowania ruchu sieciowego np. wykonywanego przez określone oprogramowanie na ściśle wskazanych

---

86 Por. E. Day, R. Bryant, *Law and Digital Crime* w: R. Bryant, S. Bryant, Policing Digital Crime, Wyd. Ashgate, Anglia 2014, s. 84 i nast.

87 Prezentowany podział stanowi swoiste rozwinięcie koncepcji dyferencjacji dowodów elektronicznych na pozyskiwane w czasie rzeczywistym oraz dowody w pozyskiwane w fazie przechowywania, prezentowanej m. in. przez A. Lach w: Dowody cyfrowe..., op. cit., s .2.

portach sieciowych - stają się źródłami dowodowymi w całości bądź też w części odseparowanymi od cyberprzestrzeni (to jest wchodzącymi w skład kategorii pierwszej). Dodatkowo, wiele spośród materiałów przetwarzanych za pośrednictwem sieci (jak choćby wiadomości poczty e-mail) po ich przesłaniu przez sieć, zapisują się lokalnie w systemach w postaci trwałej bądź też tymczasowej kopii. W efekcie, możliwa jest ustawiczna „migracja" materiału pomiędzy wskazanymi kategoriami źródeł, które w żadnej mierze nie wykluczają się, zaś krzyżują, stanowiąc nierzadko wzajemne uzupełnienie (jak w przykładzie z pocztą elektroniczną, która zapisuje się na serwerze oraz następnie jest pobierana na komputer co nie musi wiązać się z jej usunięciem z serwera pocztowego).

Powyższy podział źródeł dowodowych na źródła lokalne oraz sieciowe, pozwala natomiast zaznaczyć problematykę ścisłego określania systemów teleinformatycznych oraz innych urządzeń elektronicznych, na których możliwe będzie zabezpieczenie danego materiału dowodowego oraz następnie określania niezbędnych narzędzi i środków do przeprowadzenia takiego zabezpieczenia. O ile bowiem materiały przechowywane w danym czasie wyłącznie lokalnie możliwe są do pozyskania jedynie przy fizycznym kontakcie z nośnikiem, na którym są zapisane, czy też systemem, na którym są przetwarzane, o tyle materiały występujące w sieci, możliwe są do uzyskania także za pośrednictwem tejże sieci, w ramach ich odczytania oraz utrwalenia *on-line*.

Stosując podział wyłącznie typologiczny[88] - podyktowany opisanymi względami technicznymi umożliwiającymi fizyczną lokalizację materiału, w ramach pierwszej spośród wymienionych kategorii źródeł dowodów elektronicznych wskazać można *inter alia* na następujące rodzaje urządzeń oraz nośników[89]:

1) komputery stacjonarne - wykorzystujące całą gamę nośników oraz pamięci, jak:
    a) dyski twarde,
    b) wymienne nośniki danych,
    c) pamięci ulotne - stanowiące często jedyne źródło materiału niezapisanego w sposób trwały, którego poprawne zabezpieczenie wymaga szczególnej ostrożności (np. wyłączenie komputera powoduje usunięcie zapisów pamięci podręcznej RAM, co może prowadzić do bezpowrotnego usunięcia np. pisanego lecz niezachowanego pliku tekstowego),

[88] W oparciu o prezentowane w literaturze z zakresu informatyki śledczej typowe źródła dowodów elektronicznych, np. E. Casey, op. cit., s. 437 i nast., czy M. C. S. Lange, K. M. Nimsger, op. cit., s. 153 i nast.

[89] Por. I. Kennedy, E. Day, *Procedures at Digital Crime Scenes* w: R. Bryant, S. Bryant, *Policing Digital Crime*, Wyd. Ashgate, Anglia 2014, s. 149 i nast.

   d) pamięci układu BIOS (w uproszczeniu układ rozruchowy komputera) itd.;
2) komputery przenośne - o zakresie zastosowania analogicznym jak w przypadku komputerów stacjonarnych;
3) zewnętrzne dyski twarde służące do trwałego przechowywania dużych ilości danych (np. kopii zapasowych, czy materiałów archiwalnych), w tym tzw. dyski bezprzewodowe (działające np. w oparciu o interfejs Wi-Fi) oraz dyski podłączone do urządzeń sieciowych (np. bezprzewodowych routerów umożliwiających współdzielenie danego dysku);
4) nośniki optyczne (wszelkiego rodzaju płyty);
5) przenośne pamięci USB lub też pamięci wykorzystujące inne technologie interfejsu;
6) karty pamięci;
7) pamięci wbudowane w drukarkach oraz tzw. urządzeniach wielofunkcyjnych (pamięci te służą do kolejkowania wydruków, bądź też skanów);
8) pamięci wbudowane lub zainstalowane w telefonach komórkowych, tabletach, odtwarzaczach mp3, aparatach fotograficznych, czy kamerach (pamięci te mogą służyć nie tylko do przenoszenia utworów lub nagrań, ale również zwykłych dokumentów tekstowych, nawet jeśli dany typ urządzenia nie pozwala na ich obróbkę);
9) pamięci zainstalowane w urządzeniach sieciowych - modemach, routerach itd. pozwalające na przechowywanie konfiguracji tychże urządzeń, ich haseł dostępowych, list urządzeń dopuszczonych do komunikacji, czy wreszcie logów zawierających historię udanych / nieudanych zalogowań do sieci oraz ewentualnie także historię samego ruchu sieciowego;
10) pamięci urządzeń multimedialnych, jak odtwarzacze, czy konsole do gier.

Do drugiej spośród wyżej wymienionych kategorii źródeł dowodów elektronicznych - odnoszącej się do szeroko rozumianych zasobów cyberprzestrzeni, zaliczyć należy w szczególności następujące technologie sieciowe:

1) serwery - czyli komputery służące do obsługi połączeń sieciowych, *hostowania* stron internetowych (utrzymywania ich na udostępnianej w Internecie powierzchni dyskowej), realizacji usług sieciowych, jak np. prowadzenia sklepów internetowych, banków elektronicznych itd.;

2) macierze dyskowe - budowane przez dziesiątki dysków twardych, stanowiące podstawowy sposób przechowywania dużych ilości danych na potrzeby pracy serwerów;
3) wszelkiego rodzaju sieciowe urządzenia infrastrukturalne - węzły sieciowe, centrale łącznościowe, urządzenia komutacyjne, przełączniki, itd.;
4) łącza fizyczne - światłowody, kable ethernetowe itd. (łącza, stanowiące jedynie medium transmisji, nie przechowują co prawda danych, jednak umożliwiają ich przejęcie w trakcie przekazu w ramach szeroko rozumianego podsłuchu);
5) urządzenia łączności radiowej oraz transmisja radiowa - w szczególności bezprzewodowe punkty dostępowe oraz bezprzewodowe połączenia urządzeń skojarzonych.

Pomimo, iż rozróżnienie źródła dowodów elektronicznych na lokalne oraz znajdujące się w cyberprzestrzeni nie wpływa - co było juz podkreślane, na istotę tychże dowodów (np. domowy komputer stacjonarny oraz serwer sieciowy *de facto* korzystają z kompatybilnych lub wręcz tych samych rozwiązań sprzętowych oraz programowych, zaś pliki przetwarzana są w znakomitej większości w standardowych formatach), nie do pominięcia wydaje się możliwość naniesienia na powyższy podział źródeł dowodów także ich przykładowych form, właściwych typowo dla materiałów przetwarzanych lokalnie oraz tzw. zasobów sieciowych. Skonstruowane w ten sposób ujęcie dwu-pozimowe (I. nośnik, II. zapisany na nim materiał) pozwala na zobrazowanie typowych zależności: rodzaj dowodu - rodzaj nośnika.

Do typowych dowodów, które mogą być pozyskiwane w systemach pracujących lokalnie, należy zaliczyć w szczególności:

1) pliki tekstowe - dokumenty, faktury elektroniczne, notatki;
2) arkusze kalkulacyjne - zestawienia, księgi przychodów - rozchodów;
3) bazy danych;
4) wpisy do kalendarza;
5) kontakty - zapisane numery komunikatorów sieciowych;
6) kopie oprogramowania - zarówno w wersji już zainstalowanej, jak też pliki instalacyjne;
7) pliki multimedialne - zdjęcia, nagrania, kopie utworów muzycznych oraz filmów.

Pośród typowych materiałów dowodowych, które możliwe są do zabezpieczenia w systemach sieciowych, zaliczyć można natomiast:

1) dane o ruchu sieciowym - w szczególności dane identyfikujące nadawcę oraz adresata transmisji oraz jej treść, np. treść wiadomości, zawartość przekazywanego pliku lub też wydawane polecenie służące do przeprowadzenia ataku sieciowego;
2) materiały zapisane na stronach internetowych - treści tekstowe, załączone pliki, grafiki itd.;
3) wpisy na stronach internetowych, portalach społecznościowych oraz forach, zarówno otwartych publicznie, jak też zamkniętych, dostępnych wyłącznie dla ściśle określonego kręgu adresatów;
4) zasoby występujące w sieciach „ukrytych" - np. zasoby dostępne w sieci TOR;
5) wiadomości poczty elektronicznej przechowywane na serwerach pocztowych oraz transmitowane przez węzły sieci Internet;
6) komunikaty przekazywane za pośrednictwem programów sieciowych (np. Skype, ICQ, gadu-Gadu itd.);
7) komunikaty wymieniane przez użytkowników tzw. usługi *chat*;
8) komunikaty wymieniane przez użytkowników usług sieciowych, np. sieciowego komunikatora zintegrowanego z portalem Facebook, czy usługą Gmail.

PODSUMOWANIE

Podsumowując rozważania zawarte w niniejszym rozdziale należy zauważyć, że:

- istotą dowodu elektronicznego jest jego szczególna forma wyrażająca się w elektronicznym zapisie, nie pozwalającym na odczyt treści materiału bez zastosowania stosownego urządzenia do przetwarzania informacji, w szczególności systemu teleinformatycznego,
- dowodem elektronicznym jest nie tyle sam zapis materiału, czy też nośnik, na którym dany zapis widnieje, lecz określona treść. Fizyczny zapis danych na nośniku stanowi swoisty substrat materialny dowodu elektronicznego, podobnie jak kartka papieru dla dokumentu;
- z uwagi na elektroniczna formę zapisu, analizowane dowody mogą być bezstratnie powielane, przenoszone oraz transmitowane poprzez sieci. Dowody te nie ulegają też z czasem uszkodzeniu;
- dowody elektroniczne mogą przybierać różne postaci - zapisów plików tekstowych, czy multimedialnych, wiadomości pocztowych, plików oprogramowania, historii

ruchu sieciowego, wpisów na stronach WWW, forach, portalach społecznościowych, operacji wykonywanych przy wykorzystywaniu usług sieciowych itd.,

- dowody elektroniczne z punktu widzenia technicznego mogą być pozyskiwane zarówno poprzez fizyczne zabezpieczanie nośników danych wykorzystywanych w systemach pracujących lokalnie lub w sieci, jak również w ramach zabezpieczania materiałów przetwarzanych *on-line* (czy to zapisanych w szeroko rozumianych zasobach cyberprzestrzeni, czy też w czasie ich transmisji poprzez kolejne węzły sieci).

Rozdział VI
Transpozycja czynności procesowych do obszaru cyberprzestrzeni

§1. Zakres transpozycji dowodowych czynności procesowych do świata cyberprzestrzeni

Zgodnie z przyjętą konstrukcją pracy, niniejszy rozdział poświęcony został kwestii podejmowania dowodowych czynności procesowych w obszarze cyberprzestrzeni. Z uwagi na specyfikę domeny cyfrowej, ale także fakt, iż oryginalna konstrukcja prawna czynności procesowych tworzona była z myślą o czynnościach podejmowanych w otaczającej nas *fizycznej* rzeczywistości - analiza prawna przedmiotowego zagadnienia stanowi istotne wyzwanie, łącząc w sobie dorobek wszelkich dotychczasowych rozważań, w tym zarówno prawnych, jak i *quasi* technicznych. Przedmiotowa problematyka generuje bowiem zupełnie nowe problemy, przed którymi coraz częściej staje jednak współczesny wymiar sprawiedliwości. Co warto podkreślić, analiza poruszanych w tym miejscu kwestii procesowych pozwala nie tylko na wzbogacenie pracy o kolejny obszar tematyczny, ale także na prezentację cyberprzestępczości w ujęciu dynamicznym, uzupełniając ponadto dotychczasowe rozważania o istocie samej cyberprzestrzeni. W ocenie autora - niniejszy rozdział stanowi zatem swoisty punkt zborny dla tematyki całej pracy, skupiający uwagę na najtrudniejszych dla prawników zajmujących się obszarem cyberbezpieczeństwa kwestiach podejmowania czynności procesowych w *cyber-rzeczywistości*. Jednocześnie, z uwagi na liczbę szczególnych cech charakteryzujących zarówno metodykę techniczną, jak i specyfikę kwalifikacji prawnej podejmowania czynności procesowych w obszarze domeny cyfrowej, nie jest możliwe mówienie w tym miejscu o stosowaniu prostej analogii. *De facto*, mając na uwadze wszelkie odrębności różniące *rzeczywistości*: *fizyczną* oraz *cyber* - niezbędne staje się aktualnie mówienie o transpozycji tradycyjnych, dowodowych czynności procesowych do nowego, komputerowego wymiaru ludzkiej aktywności, jakim jest właśnie cyberprzestrzeń[1].

Powyższe zagadnienie podzielone zostało na dwie części, poświęcone odpowiednio:

[1] Zagadnienie to szeroko identyfikowane jest w piśmiennictwie amerykańskim, np: M. C. S. Lange, K. M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know*, Wydawnictwo *American Bar Association*, Chicago 2009, E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Elsevier, Massachusetts 2011, M. Cross, D. Littlejohn Shinder, *Scene of the Cybercrime*, Syngress 2008, A. Reyes, *Cyber Crime Investigations*, Elsevier, USA, 2007, czy też H. M. Jarrett, M. Bailie, E. Hagen, N. Judish, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Ministerstwo Sprawiedliwości USA 2009.

I. ogólnej transpozycji czynności procesowych do świata cyberprzestrzeni (kwestie zdefiniowania czynności procesowej w obszarze cyberprzestrzeni, określenia *miejsca* realizacji czynności, prawa właściwego dla jej przeprowadzenia, dopuszczalnych granic prawnych działania oraz faktycznego przedmiotu czynności dokonywanej w rzeczywistości zbudowanej z bitów, to jest ciągów zer i jedynek); oraz,

II. szczególnej analizie problematyki podejmowania w cyberprzestrzeni czynności przeszukania oraz zatrzymania rzeczy (w szczególności kwestie zakresu oraz zasięgu tych czynności, a także możliwości faktycznych oraz prawnych ich podejmowania na odległość bez bezpośredniego - fizycznego kontaktu z informatycznym nośnikiem danych zawierającym pozyskiwane dowody).

Rozdział zakończony jest podsumowaniem zawartych w nim rozważań oraz przedstawieniem szeregu postulatów *de lege lata*, których wprowadzenie wydaje się niezbędne dla uniknięcia podstawowych wątpliwości nasuwających się na tle realizacji celów procesu karnego w ramach podejmowania czynności w niematerialnym oraz bezkształtnym świecie cyberprzestrzeni.

Jak zostało zauważone powyżej, obowiązujące już od wielu lat przepisy Kodeksu postępowania karnego regulujące problematykę podejmowania czynności procesowych, tworzone były z myślą o specyfice działania w ramach otaczającej nas *fizycznej* rzeczywistości. W szczególności, w zakresie pozyskiwania materiału dowodowego w postaci dowodów rzeczowych, regulacje kodeksowe oparto na założeniu, iż materiały te przejawiają się zawsze w postaci skonkretyzowanych przedmiotów, posiadających w efekcie - jak każda materia - swoje fizyczne wymiary, np. długość, objętość, czy też wagę, określony stan fizyczny (stały, ciekły lub gazowy), a także ściśle oznaczalną lokalizację. Mając jednak na uwadze wcześniejsze - zawarte w rozdziałach II. i III. niniejszej pracy, rozważania na temat specyfiki oraz budowy cyberprzestrzeni, a także prowadzone na gruncie rozdziału VI. badania nad istotą dowodów elektronicznych, należy jednoznacznie stwierdzić, iż cechy te nie odnoszą się do *substancji świata* cyberprzestrzeni, nie pozwalając na kwantyfikowanie danych komputerowych budowanych przez przecież nieskończenie długie ciągi bitów informacji, wyrażanych przez logiczne zera i jedynki. Uzupełniając tak zarysowany obraz, warto przypomnieć, iż owe ciągi dwuwartościowych znaków na najniższym poziomie technicznym reprezentowane są w szeroko rozumianych systemach teleinformatycznych wyłącznie poprzez różnice wysokości napięcia elektrycznego występującego w układach przetwarzających dane, w szczególności zaś procesorze (CPU), układzie graficznym (GPU)

oraz pamięci (w przypadku komputerów w szczególności pamięci operacyjnej RAM oraz pamięci podręcznej tzw. CACHE). Dodatkowo, w trakcie trwałego magazynowania danych, bity informacji mogą być zapisywane także w postaci optycznej (ścieżki tzw. *pitów i landów*[2] fizycznie wypalone na płytach CD, DVD, BluRay itd.) lub też magnetycznej (zapis na dyskach twardych, tzw. HDD) - choć formy te stanowią jedynie sposób przechowywania danych, które na potrzeby ich dalszego przetwarzania (a w szczególności odczytu) muszą ponownie zostać przekształcone do postaci impulsów elektrycznych występujących w stosownych podzespołach urządzeń cyfrowych.

Przedstawiona w niniejszej pracy specyfika obszaru cyberprzestrzeni oraz dowodu elektronicznego zarysowuje szereg zagadnień problemowych wpływających bezpośrednio na sposób nie tylko prowadzenia czynności procesowych wewnątrz cyberprzestrzeni lub wobec jej zasobów i składników, ale przede wszystkim - na sam sposób pojmowania istoty prowadzenia tychże czynności w obszarze domeny cyfrowej. Wskazując - w tym miejscu jedynie sygnalnie, na jaskrawe przykłady sposobu, w jaki owa specyfika świata cyfrowego wypaczyła tradycyjne rozumienie mechanizmów prawnych podejmowania czynności procesowych - przywołać można choćby:

- fakt bezstratnego oraz często w pełni zautomatyzowanego powielania danych mogących stanowić materiał dowodowy[3] (powielanie stanowi często utrwalony sposób funkcjonowania systemów teleinformatycznych - np. wysyłając *e-mail* w istocie wysyłamy kopię danych sporządzonych na komputerze nie zaś ich *jedyny egzemplarz*, jak w przypadku nadania tradycyjnej poczty w zaklejonej kopercie), czy też,
- problematykę możliwości podejmowania czynności procesowych „zdalnie"[4], to jest za pośrednictwem sieci, po uzyskaniu dostępu *on-line* do zasobów mających zostać poddanych zabezpieczeniu (czyli w istocie - skopiowaniu oraz utrwaleniu w odpowiedniej formie w pamięci, czy też na informatycznym nośniku danych,

---

[2] Więcej o zapisie optycznych nośników danych na stronach internetowych dostępnych pod adresami: http://pl.wikipedia.org/wiki/Dyski_CD, http://pl.wikipedia.org/wiki/DVD oraz http://pl.wikipedia.org/wiki/Blu-ray, a także http://pl.wikipedia.org/wiki/Pit oraz http://pl.wikipedia.org/wiki/Land_(dyski_optyczne).

[3] Kwestia coraz częściej zaznaczana w piśmiennictwie, tak np. J. Błachut, Dokument jako przedmiot ochrony prawnokarnej, Lex, Warszawa 2011, s. 126, czy A. Lach, Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia teoretyczne i praktyczne, e-biuletyn CBKE 2/2004, Wrocław 2004, s. 4. Tekst opracowania dostępny jest na stronie internetowej pod adresem: http://www.bibliotekacyfrowa.pl/Content/24720/Dowody_cyfrowe_w_postepowan.pdf.

[4] Na kwestię tę szczególną uwagę zwraca A. Adamski w: Przestępczość w cyberprzestrzeni, prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy, Dom Organizatora, Toruń 2001, s. 129.

komputera lub innego urządzenia teleinformatycznego wykorzystywanego w realizacji czynności).

Mając powyższe na uwadze, do zagadnień, których przybliżenie wydaje się niezbędne dla wyczerpania zakresu uwag ogólnych odnoszących się do transpozycji dowodowych czynności procesowych do świata cyberprzestrzeni - należy w konsekwencji zaliczyć w szczególności:

1) próbę określenia przedmiotu czynności dowodowej podejmowanej w cyberprzestrzeni oraz wynikające stąd następstwa dla sposobu prowadzenia takich czynności;
2) próbę określenia lokalizacji przedmiotu czynności procesowej podejmowanej w cyberprzestrzeni z punktu widzenia procesowego;
3) korelację dowodowych czynności procesowych podejmowanych w cyberprzestrzeni z tradycyjnymi formami dowodowymi, podejmowanymi już poza cyberprzestrzenią, ale w odniesieniu do czynu popełnionego w jej obszarze;
4) kwestię dopuszczalnego prawnie oraz możliwego technicznie zasięgu realizacji czynności procesowych podejmowanych w obszarze cyberprzestrzeni;
5) kwestię bezstratnej duplikacji dowodów elektronicznych z punktu widzenia procesowego; oraz,
6) próbę ustalenia prawa właściwego dla dokonania czynności procesowej podejmowanej w *bez-terytorialnej* cyberprzestrzeni.

Wymienione w powyższym katalogu zagadnienia zostały zaprezentowane w kolejnych podpunktach rozdziału z zachowaniem przedstawionego toku prowadzenia wywodu. Celem uniknięcia powtórzeń rozważań prowadzonych na gruncie poprzednich rozdziałów pracy, dalsze uwagi zostały skupione na kwestiach *stricte* procesowych.

1. Określenie przedmiotu czynności dowodowej podejmowanej w cyberprzestrzeni

Zgodnie z przepisami obowiązującego Kodeksu postępowania karnego[5], celem nadrzędnym prowadzenia postępowania dowodowego w ramach procesu karnego jest zapewnienie, aby wszystkie okoliczności faktyczne danej sprawy zostały możliwie jednoznacznie wyjaśnione - a w konsekwencji, by sprawca ujawnionego przestępstwa został wykryty oraz pociągnięty do odpowiedzialności karnej z jednoczesnym zapewnieniem

[5] Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, Dz. U. Nr 89, poz. 555, z późn. zm.

ochrony osób niewinnych[6] (*vide* w szczególności art. 2 § 1 pkt 1 oraz § 2, art. 4, czy też art. 170 Kpk). Powyższy postulat stanowi jedną z naczelnych zasad współczesnego procesu karnego, kierunkując działania organów ścigania na poznanie rzeczywistego przebiegu przestępstwa (tzw. prawdy materialnej) oraz oferując gwarancję rzetelności oraz bezstronności całego wymiaru sprawiedliwości[7]. Co istotne, stanowiąc o badaniu „okoliczności faktycznych", przywołana dyrektywa Kodeksu postępowania karnego w żadnym razie nie zawęża zakresu przedmiotowego działań nastawionych na poznanie prawdy o popełnionym czynie, nie tylko zezwalając, ale wręcz nakazując podejmowanie czynności śledczych w możliwie szerokim zakresie - *de iure* ograniczonym wyłącznie regułami legalności oraz w wąskim zakresie - ekonomiki realizacji poszczególnych czynności, stanowiącej przejaw zasady oportunizmu. W szczególności jednak – wskazana wyżej dyrektywa procesowa obejmuje nie tylko prowadzenie ustaleń faktycznych w sferze *rzeczywistości fizycznej*, ale także dokonywanie wyjaśnień w obszarze cyberprzestrzeni. Innymi słowy - o ile tylko cyberprzestrzeń oraz zawarte w niej informację mogą stanowić źródło relewantnego dla sprawy materiału dowodowego - o tyle skorzystanie ze wskazanych zasobów stanowi obowiązek prawny organów ścigania prowadzących dane postępowanie karne.

Co było podkreślane w poprzednich częściach pracy - w szczególności zaś w rozdziałach poświęconych definicji oraz budowie cyberprzestrzeni, a także w rozdziale charakteryzującym istotę dowodów elektronicznych, swoistą tkanką domeny cyfrowej są omalże nieskończone ciągi bitów informacji, składające się na dane komputerowe przetwarzane przez systemy teleinformatyczne na poziomie lokalnym lub też w ramach ruchu sieciowego o potencjalnie globalnym zasięgu. Niezależnie od formy prezentacji owych danych - mogących występować w systemach czy to w postaci tekstowej (np. wszelkiego rodzaju dokumenty, arkusze kalkulacyjne, kopie wiadomości poczty elektronicznej, zapisy komunikatów przekazywanych na czatach lub w komunikatorach itd.), graficznej, audiowizualnej, czy też w postaci kodu (skompilowanego lub źródłowego) programów komputerowych, czy wreszcie w postaci informacji opisujących sam ruch sieciowy (tzw. logi) - na poziomie pracy systemów, dane te nadal pozostają zbitkami bitów informacji, dających zapisać się poprzez frazy dwuwartościowych zer i jedynek. W tym sensie, każda czynność dowodowa podejmowana *wewnątrz* obszaru cyberprzestrzeni będzie miała za przedmiot *de*

[6] Zasada tzw. trafności reakcji karnej podejmowana jest szeroko przez A. Gaberle w: Dowody w sądowym procesie karnym, Oficyna, Warszawa 2010, wyd. 2, s 23 i nast., czy też S. Waltoś, Proces karny. Zarys systemu, Lexis Nexis, Warszawa 2009, wyd. 10, s. 24 i nast. oraz 219 i nast.

[7] Proces karny: część ogólna, G. Artymiak, Z. Sobolewski, Wolters Kluwer Polska, 2007, s. 34.

facto określoną porcję danych komputerowych - które w czasie prowadzenia czynności mogą być zarówno przechowywane na określonym informatycznym nośniku danych (a zatem wyłącznie w postaci statycznej), właśnie przetwarzane w systemie (w tym wytwarzane) lub też przekazywane/odbierane za pośrednictwem lokalnych bądź rozległych sieci komputerowych, w szczególności zaś sieci Internet.

Charakteryzowane powyżej dane komputerowe zapisywane są w systemach teleinformatycznych najczęściej w postaci plików komputerowych (w tym plików bazodanowych), definiowanych przykładowo jako „uporządkowany zbiór danych, o skończonej długości, posiadający szereg atrybutów"[8]. Nazywane także „zasobami do przechowywania informacji"[9], pliki komputerowe charakteryzuje relatywna trwałość, rozumiana jako niezmienność w czasie, gdy zapisany plik nie jest poddawany obróbce - np. edycji, w określonym programie komputerowym. Warto zaznaczyć, iż co do zasady, jeden plik może w danym czasie stanowić przedmiot operacji tylko jednego programu komputerowego, co może powodować istotne - opisane dalej, trudności w realizacji czynności procesowych dokonywanych w obszarze cyberprzestrzeni. Szczególnym rodzajem plików komputerowych są tzw. katalogi, które zawierając listy plików, pozwalają na ich wygodne sortowanie, lokalizowanie oraz poddawanie zbiorczym operacjom - obejmującym swoim zakresem całą zawartość katalogu. Podstawowym elementem budowy każdego pliku jest jego rozszerzenie (z ang. *file extension*[10]) określające rodzaj pliku (plik tekstowy, graficzny, bazodanowy, archiwum itd.) oraz wskazujące na program właściwy do jego obsługi. Rozszerzenie pliku zapisywane jest najczęściej w postaci trzech liter następujących po nazwie pliku, po oddzieleniu kropką (np. popularnie stosowana nazwa pliku informacyjnego *readme.txt*). Do najczęściej występujących rozszerzeń plików zaliczyć można:

– *.exe* - plik wykonywalny programu komputerowego, gry (*executable*),
– *.doc* - dokument tekstowy (może zawierać wplecione grafiki) sporządzony według standardu firmy Microsoft (w szczególności wytworzony w programie Word pakietu Microsoft Office, ale także w programach otwartych, jak np. Open Office),
– *.pdf* - dokument tekstowy sporządzony według standardu określonego przez firmę Adobe,

8 Tak np. na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/Plik.
9 Za charakterystyką pliku przedstawioną na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Computer_file.
10 Więcej na temat rozszerzeń na stronach internetowych dostępnych pod adresami: http://www.bbc.co.uk/webwise/guides/file-extensions, czy też http://en.wikipedia.org/wiki/Filename_extension.

- *.jpg* - plik graficzny, np. zdjęcie, grafika komputerowa,
- *.gif* - plik graficzny o ograniczonej palecie kolorów, dzięki wyświetlaniu sekwencyjnemu mogący zawierać krótkotrwały (maksymalnie kilkusekundowy) film niemy,
- *.avi, .wmv* - pliki filmowe z możliwością zapisu dźwięku,
- *.mp3* - plik dźwiękowy, np. utwór muzyczny, ale także nagranie dźwięku z dyktafonu,
- *.txt* - prosty plik tekstowy, poddawany edycji z zastosowaniem podstawowych narzędzi systemowych,
- *.zip* - plik archiwum, zawierający inne pliki poddane tzw. kompresji, czyli procesowi obniżania objętości kosztem ich tymczasowego „zamrożenia" (pliki skompresowane nie mogą być normalnie wykorzystywane do czasu ich dekompresji); pliki archiwum mogą być zabezpieczone hasłem do ich dekompresji,
- *.db* - przykładowy plik bazodanowy, zawierający w sobie kompletny lub częściowy zapis bazy danych,

oraz podstawowe rozszerzenia plików budujących strony internetowe:

- *.html* - pliki zapisane w języku programowania *hypertext markup language*, oraz,
- *.php* - pliki zapisane w języku *personal home page*, zawierające aktywne skrypty wykonywane po stronie serwera (strona napisana w języku php *de facto* buduje się od nowa za każdym razem, gdy jest otwierana przez Internet).

Nazwa pliku - czyli zawsze widoczne dla użytkownika określenie pliku (w pełnym zapisie poprzedzające jego rozszerzenie), nadawana jest natomiast swobodnie, bądź to przez samego użytkownika, bądź też automatycznie przez program komputerowy przetwarzający dany plik. Jedynymi ograniczeniami w budowaniu nazwy pliku są: określona długość znaków (np. w systemach z rodziny Microsoft Windows, opartych na systemie plików NTFS, liczba ta wynosi 255 znaków[11]) oraz zakaz stosowania w nazwie niektórych znaków, np. diakrytycznych, znaku zapytania, czy też w niektórych systemach operacyjnych, znaku kropki - zarezerwowanej dla pełnienia funkcji rozdziału nazwy od rozszerzenia. Wskazując na typowe nazwy plików, występujące najczęściej w określonych sytuacjach, można zauważyć, że typową nazwą nadawaną dla pliku tzw. strony głównej witryny internetowej, jest wyraz *index* (*index.html* lub *index.php*). Pliki instalacyjne programów komputerowych przybierają natomiast najczęściej brzmienie *setup.exe,* czy *install.exe*. Należy jednak

[11] Zestawienie dopuszczalnych długości plików w różnych systemach zapisu plików można znaleźć na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Comparison_of_file_systems#Limits.

pamiętać, iż zarówno nazwa pliku, jak również jego rozszerzenie, mogą zostać w każdej chwili zmienione przez użytkownika - co istotne, z wykorzystaniem wyłącznie podstawowych narzędzi wbudowanych w każdy system operacyjny. Tym samym, plik „udający" uszkodzony dokument tekstowy (np. o nazwie *rachunek-PGE.doc* może w istocie być zaszyfrowanym archiwum, czy też zaszyfrowanym kontenerem[12]).

Kończąc opis budowy plików - będących w istocie podstawowym „źródłem" dowodów elektronicznych (pliki stanowią bowiem swoisty budulec dla dowodów elektronicznych), należy również zauważyć, iż jednym z dostępnych atrybutów systemowych plików jest ich tzw. „ukrywanie", powodujące możliwość prostego chowania plików przed oczami użytkownika systemu. Ukrywanie stosowane jest na przykład domyślnie w wielu systemach operacyjnych w stosunku do plików, których nieumyślne uszkodzenie mogłoby spowodować awarię całego systemu, w tym jego permanentne uszkodzenie. Pliki ukryte nie wyświetlają się w trakcie przeglądania katalogów, dopóki nie zostaną ustawione stosowne opcje wyświetlania zawartości folderów wraz z plikami ukrytymi. Tym samym, poszukiwania określonego pliku nie mogą ograniczać się do zwykłego „poszukiwania wzrokowego", lecz są dokonywane przede wszystkim w sposób zautomatyzowany, przy zastosowaniu specjalistycznych narzędzi programowych oraz sprzętowo-programowych.

Z punktu widzenia procesowego, niezwykle istotną cechą plików jest ich integralność (często nazywana też „spójnością"). Cecha ta w języku informatycznym oznacza swoistą *oryginalność* pliku, odnosząc się do faktu, iż dany plik nie został zmieniony w sposób nieuprawniony oraz zachował swoją pierwotną budowę, nadaną mu przez jego wytwórcę[13]. Nieco na marginesie, warto w tym miejscu zaznaczyć, iż nie wszystkie pliki powstające w pamięci komputera wytwarzane są bezpośrednio przez użytkownika, lecz mogą stanowić także wytwór samego systemu. Sytuacja taka ma miejsce w przypadku plików tworzonych automatycznie - jak choćby wielokrotnie przywoływane logi systemowe, ale także np. pliki zawierające dane podpisu elektronicznego. Pliki takie stanowią pośredni efekt działań człowieka - jak np. wynik złożenia podpisu elektronicznego, często stanowiąc

[12] Uzupełniająco na temat szyfrowania danych: D. E. Denning, W. E. Baugh, *Hiding crimes in cyberspace* w: D. Thomas, B. D. Loader, *Cybercrime. Law enforcement, security and surveillance in the information age,* Wyd. Routledge, Londyn 2000, s. 106 i nast. Należy zauważyć, iż w sieci dostępnych jest wiele darmowych technologii służących do tworzenia tzw. szyfrowanych kontenerów, czyli zabezpieczonych systemów plików, zawierających w swoim wnętrzu dowolną liczbę zaszyfrowanych plików. Niezależnie od wielkości poszczególnych plików zamkniętych w kontenerze, kontener może posiadać wielkość dowolnie większą niż suma plików wchodzących w jego skład. Dzięki takiej budowie, przy próbie nieuprawnionego otwarcia kontenera, użytkownik otrzymuje wyłącznie zaszyfrowany oraz dodatkowo zmieszany materiał.

[13] Więcej na temat pojęcia na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/Integralno%C5%9B%C4%87_danych.

nieuświadamiany ślad cyberprzestępstwa. Cecha integralności plików (danych zawartych w plikach) pozostaje w bezpośrednim styku z zasadami postępowania dowodowego, którego celem jest zapewnienie, iż zbierane dowody są autentyczne oraz nie zostały zniekształcone - lub co gorsza zmienione, w trakcie podejmowanych wobec nich czynności procesowych. W konsekwencji jej funkcjonowania, jakiekolwiek operacje dokonywane na plikach w czasie ich zabezpieczania - takie, jak np. robienie wyciągów z plików (np. ekstrakcja jednej wiadomości poczty elektronicznej z wielostronicowego pliku archiwum poczty), czy wręcz tworzenie nowych plików z danych zawartych w zabezpieczanym materiale, powodują istotne zmiany plików, manifestujące się choćby w dacie ostatniej modyfikacji pliku (data ta zapisywana jest w postaci tzw. *metadanych* pliku)[14]. Co oczywiste, plik zmodyfikowany już po jego zabezpieczeniu w systemie sprawcy traci swoją wartość dowodową, stając się jednocześnie podatnym na zarzut jego sfałszowania lub uszkodzenia[15]. W następstwie powyższego, nawet gdy wystarczającym dowodem popełnienia cyberprzestępstwa może być już fragment pliku komputerowego, konieczne jest i tak zabezpieczenie jego całości, celem wykluczenia naruszenia cechy integralności zabezpieczanych danych. Samo zabezpieczanie materiału poprzez jego kopiowanie[16] musi być natomiast dokonywane z zastosowaniem specjalistycznych rozwiązań sprzętowo - programowych (tzw. blokerów), zapobiegających możliwości pojawienia się jakichkolwiek zmian w powielanym pliku[17] (jak choćby wpisaniu nowej, zaktualizowanej daty jego ostatniej modyfikacji w postaci powielenia).

Z punktu widzenia prawnego, pliki stanowią elektroniczne *ucieleśnienie* określonych praw użytkowników oraz ich wytwórców. Przykładowo, pliki graficzne stanowią najczęściej przedmiot majątkowych praw autorskich zawierając w sobie cyfrowy zapis zdjęcia, grafiki, projektu strony internetowej itd., które stanowią dzieło w myśl zasad zarówno krajowego, jak i międzynarodowego prawa autorskiego. Co należy podkreślić, fakt zapisu zdjęcia, piosenki, czy też całej książki w postaci elektronicznej, w żadnej mierze nie zmienia ani istoty przedmiotu, który został zapisany w pliku, ani zasad jego ochrony, wyrażonych w generalnych przepisach prawa.

Obok ochrony praw autorskich, pliki komputerowe podlegają oczywiście także ochronie przewidzianej w przepisach właściwych z punktu widzenia treści danego pliku, np. przepisach prawa ochrony danych osobowych, czy przepisach o ochronie tajemnic -

---

14 M. Cross, D. Littlejohn Shinder, *Scene of the Cybercrime*, Syngress 2008, s. 122 i nast.
15 J. Błachut, op. cit., s. 126.
16 Por. I. Kennedy, E. Day, *Procedurs at Digital Crime Scenes* w: R. Bryant, S. Bryant, *Policing Digital Crime*, Wyd. Ashgate, Anglia 2014, s. 153 i nast.
17 M. Cross, D. Littlejohn Shinder, op. cit., s. 122 i nast.

lekarskiej, adwokackiej, bankowej, telekomunikacyjnej, ochronie informacji niejawnych itd. Wiele spośród przetwarzanych w sposób cyfrowy zasobów posiada wręcz swoje szczególne regulacje prawne, nakazujące zapewnienie odpowiednich warunków bezpieczeństwa przetwarzania danych. Za przykład mogą tu posłużyć choćby przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[18] oraz wydanego do niej rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[19], czy też przepisy ustawy o z dnia 5 sierpnia 2010 r. ochronie informacji niejawnych[20] oraz wydanego na jej podstawie rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego[21]. Z uwagi na swój szczególnych charakter odrębna regulacja prawna została stworzona także do ochrony prawnej baz danych, wyrażonej w przepisach ustawy z dnia 27 lipca 2001 r. o ochronie baz danych[22]. Zgodnie z przepisami tego aktu, przez bazę danych należy rozumieć „zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości”[23].

Co więcej - jak w odniesieniu do każdego innego dobra prawnie chronionego, do plików komputerowych należy stosować także konstytucyjne zasad ochrony praw człowieka i obywatela, w szczególności zaś zasady kreujące prawo do prywatności, czy tajemnicy korespondencji. Ponownie należy podkreślić, iż fakt występowania danych komputerowych w postaci cyfrowej w żadnej mierze nie ogranicza ochrony prawnej należnej określonej porcji danych z uwagi na ich treść. W szczególności, stanowiąc przedmiot ochrony prawnej, pliki komputerowe podlegają wszelkim rygorom karnoprocesowym, ustalającym czy to zasady prowadzenia czynności dowodowych, takich jak wydanie oraz zatrzymanie materiału dowodowego, czy też odnoszącym się do ukonstytuowania zasady swobodnej oceny dowodów. Dane komputerowe poddawane są ocenie prawnej pod kątem reprezentowanych przez nie treści - nie zaś ich formy, stanowiąc przykładowo dowody dokonywania

[18] Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.
[19] Dz. U Nr 100 poz. 1024.
[20] Dz. U. Nr 182 poz. 1228.
[21] Dz. U Nr 159 poz. 948.
[22] Dz. U. Nr 128 poz. 1402, z późn. zm.
[23] Art. 2 ust. 1 pkt 1 ustawy z dnia 27 lipca 2001 r. o ochronie baz danych.

określonego ruchu sieciowego, zapis elektronicznej postaci podrobionego dokumentu, czy nielegalną kopię utworu.

Istotną bolączką obowiązujących w zakresie dowodów elektronicznych przepisów jest natomiast brak formalnego odniesienia się w regulacjach prawnych do cyfrowego materiału dowodowego, jako materiału w istocie odrywającego się od informatycznego nośnika danych, na których dane te są zapisane. Co było podkreślane w poprzednim rozdziale - dowodami elektronicznymi nie są bowiem dyski twarde, płyty CD, bądź pamięci USB, ale zapisane na nich pliki oraz zawarte w nich treści[24]. Brak wyraźnego rozdzielenia prawnego pomiędzy nośnikiem a samym dowodem powoduje w konsekwencji konieczność traktowania, jako dowodów głównie fizycznych nośników, dających się opisać, zaewidencjonować oraz dołączyć do prowadzonych wciąż w postaci papierowej akt sprawy. Jako przykłady negatywnych konsekwencji takiego stanu wskazać można na[25]:

- istotne utrudnienia lub wręcz brak możliwości „zatrzymania" danych przetwarzanych na serwerze zlokalizowanym poza granicami kraju - choć dane pobierane z takiego serwera *on-line* poprzez sieci (np. pobrane nielegalne pliki instalacyjne płatnego oprogramowania) stanowią przecież idealne odzwierciedlenie pliku źródłowego, a więc z punktu widzenia dowodowego - materiał identyczny z tym, który zostałby zabezpieczony „na miejscu" lokalizacji serwera,
- konieczność pozyskiwania dysków twardych, których wyjęcie z systemu może uniemożliwiać dalszą pracę systemu teleinformatycznego potencjalnie narażając Skarb Państwa na odpowiedzialność finansową w przypadku podjęcia błędnych czynności procesowych lub też w przypadku działań podejmowanych w odniesieniu do komputerów samej ofiary ataku cybernetycznego (zabezpieczenie dowodów ataku może w tej sytuacji wiązać się z dodatkowym obciążeniem ofiary przestępstwa spowodowanym np. koniecznością zatrzymania na potrzeby dowodowe całej macierzy dysków przedsiębiorstwa, w którym atak został przeprowadzony),
- utrudnienia w identyfikacji, a co za tym idzie, lokalizacji informatycznych nośników danych zawierających całość lub jedynie fragmenty interesującego materiału dowodowego, spowodowane stosowaniem technologii takich jak rozległe macierze dyskowe, gdzie pojedynczy plik może potencjalnie być zapisany fragmentarycznie na wielu dyskach, czy też przetwarzaniem danych w tzw. chmurze, której infrastruktura

[24] Tak np.: A. Adamski, Prawo karne komputerowe, CH Beck, Warszawa 2000, s. 199, J. Błachut op. cit., s. 41 i nast., czy też A. Lach, Dowody cyfrowe..., op. cit., s. 1 - 2.
[25] Uwagi oparte częściowo na rozważaniach A. Lacha w: Dowody cyfrowe..., op. cit., s. 2 - 7.

może być zbudowana w oparciu o setki serwerów rozsianych po całym świecie oraz współdzielona przez dziesiątki przedsiębiorców, korzystających z usługi dostawcy chmury obliczeniowej,

- problematykę dalszego wykorzystywania przez ofiarę ataku komponentów zaatakowanego systemu teleinformatycznego - po przeprowadzeniu ataku, dany system najczęściej wykorzystywany jest dalej do prowadzenia bieżącej pracy. Praca ta powoduje z kolei nadpisywanie na dysku zawierającym dowody przestępstwa nowych danych, których czas utworzenia jest jednoznacznie późniejszy od czasu dokonania ataku, co może podważać wartość dowodową tak zmodyfikowanego już nośnika danych,
- konieczność podejmowania trudnych oraz czasochłonnych czynności o charakterze technicznym (tzw. *forensic*) dla zabezpieczenia materiału, który bardzo często można w istocie pobrać za pośrednictwem sieci Internet przy zastosowaniu podstawowych narzędzi systemowych dostępnych na każdym komputerze, czy wręcz zaprezentować na komputerze *on-line* na sali rozpraw (np. funkcjonujące nielegalne kasyno internetowe, czy portal zawierający nielegalne treści, np. pornografię dziecięcą).

Powyższe kwestie odnoszące się aspektu fizycznego pozyskiwania danych informatycznych stanowiących dowody cyberataków, pozwalają na płynne przejście do kolejnego zagadnienia rozdziału - zgodnego z zaproponowaną budową wywodu, czyli próby lokalizacji przedmiotu czynności procesowej podejmowanej w cyberprzestrzeni.

2. Określenie lokalizacji przedmiotu czynności procesowej podejmowanej w cyberprzestrzeni

Pomimo, iż cyberprzestrzeń - co było już wielokrotnie podkreślane, wymyka się kwantyfikacji z zastosowaniem *realnych* wymiarów, jak długość, czy szerokość, oraz charakteryzuje się swoją *szczególną geografią* przestrzeni logicznej, wszelkie dane przetwarzane w jej obrębie poddają się ścisłej (choć często niezwykle utrudnionej w wymiarze praktycznym) lokalizacji fizycznej w określonych elementach infrastruktury sieciowej tworzącej tkankę cyberprzestrzeni. Innymi słowy - każde dane składowane, czy też szerzej przetwarzane w szeroko rozumianych zasobach cyberprzestrzeni, znajdują się na identyfikowalnym nośniku danych - np. dane strony internetowej zapisane na przestrzeni dyskowej serwera, zaś wszystkie dane transportowane poprzez łącza sieciowe wędrują po ściśle określonych trasach, wykonując serię skoków po dających się zlokalizować węzłach

teleinformatycznych (więcej na temat budowy oraz zasad działania cyberprzestrzeni pisano w rozdziale III niniejszej pracy). O ile zatem sama cyberprzestrzeń jest *poza* - wymiarowa (przestrzeń logiczna), o tyle tworząca ją infrastruktura telekomunikacyjna oraz teleinformatyczna z wszelkimi urządzeniami zestawiającymi oraz obsługującymi połączenia, a także same łącza (nadajniki, kable, światłowody itp.) - poddają się fizycznej geolokalizacji.

Mając powyższe na uwadze, można by przypuszczać, iż niezwłoczna lokalizacja danych oraz trasy, jaką dane te pokonały pomiędzy dwoma lub większą liczbą fizycznych zakończeń sieci - powinny stanowić zadania trywialne, przeprowadzane w sposób w pełni zautomatyzowany. W końcu protokoły programowo-sprzętowe obsługujące funkcjonowanie sieci muszą dokładnie wiedzieć, jakie dane, kiedy oraz skąd i dokąd są przesyłane (w innym wypadku sieć przecież nie mogłaby działać). Z uwagi jednak na szczegółowe zasady działania sieci (np. możliwość przekierowywania ruchu poprzez serwery *proxy*), dostępność określonych narzędzi (w tym tych określanych mianem *hackerskich*), ale także najnowsze technologie sieciowe (jak choćby technologia przetwarzania danych w tzw. chmurach[26], czy też trasowanie cebulowe[27]) - tropienie danych w sieci oraz lokalizowanie wykorzystywanych do przeprowadzania ataków w cyberprzestrzeni zakończeń sieciowych stają się zadaniami skomplikowanymi, często wymagającymi ścisłej współpracy wielu krajów. Zdecentralizowana struktura Internetu - będącego podstawowym składnikiem cyberprzestrzeni, powoduje bowiem niemożliwość zapanowania organów ścigania dowolnego państwa nad całością domeny cyfrowej, a także konstytuuje brak jednolitych zasad prawnych odnoszących się do namierzania oraz zatrzymywania danych komputerowych przetwarzanych w infrastrukturze sieciowej zlokalizowanej geograficznie w różnych państwach - nierzadko oddalonych od siebie o tysiące kilometrów oraz zupełnie różnych ustrojowo i prawnie.

Podstawowym źródłem informacji na temat pochodzenia określonej porcji danych komputerowych przekazywanych za pośrednictwem sieci jest sam opis pakietu danych[28]. Jednym z głównych elementów pakietu - obok jego zawartości, są adresy IP nadawcy oraz odbiorcy. Adresy te identyfikują oczywiście nie tyle osoby: wysyłającą oraz odbierającą dane,

---

[26] Z ang. c*loud computing*. Więcej o technologii przetwarzania danych w chmurach na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Cloud_computing.

[27] Z ang. *onion routing*. Więcej o technologii trasowania cebulowego na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/Tor_(sie%C4%87_anonimowa), jak również na oficjalnej stronie projektu *TOR Project*, dostępnej pod adresem: www.tor.org. Więcej o technologii trasowania cebulowego w ujęciu przedstawienia technologii cyberprzestrzeni pisano także w rozdziale III niniejszej pracy.

[28] Więcej na temat budowy pakietów danych na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Pakiet_telekomunikacyjny. Uzupełniająco, opis mechanizmu enkapsulacji pakietów dostępny jest na stronie internetowej pod adresem: http://learn-networking.com/tcp-ip/how-encapsulation-works-within-the-tcpip-model.

lecz fizyczne zakończenia sieci, do których podłączone są maszyny biorące udział w wymianie danych. Identyfikacja zakończeń nie stanowi jednak remedium problemu tzw. atrybucji (możliwości przypisania do określonej osoby) ruchu sieciowego, w tym ataków, także z innych powodów. Nierzadko do jednego zakończenia fizycznego sieci może być podłączonych wiele komputerów, co ma np. miejsce w sytuacji stosowania technologii bezprzewodowych, jak routery Wi-Fi. Co więcej - w przypadku, gdy dane zakończenie sieci nie jest w żaden sposób zabezpieczone (np. otwarta sieć bezprzewodowa, niewymagająca hasła dostępowego do Internetu), potencjalnie jego użytkownikiem może być każdy. Podejmując próbę fizycznego zlokalizowania źródła danych przesłanych z takiego łącza jedynym efektem podjętych ustaleń staje się adres zamieszkania nieświadomego użytkownika, którego nieroztropnie udostępnione łącze sieciowe zostało wykorzystane do przeprowadzenia cyberprzestępstwa. W aktualnym stanie prawnym żaden przepis nie reguluje kwestii dostępności takich łączy, jak również ewentualnego zapisywania historii tzw. lokalnego ruchu sieciowego - a więc ruchu występującego już poza infrastrukturą dostawcy usług sieciowych. Dostawcy ci - inaczej niż osoby fizyczne, jako przedsiębiorcy świadczący profesjonalnie usługi łącznościowe zobligowani są do zachowywania danych o ruchu sieciowym w ramach tzw. szeroko rozumianej retencji danych (o czym więcej w dalszej części rozdziału).

Z uwagi na sygnalizowane już wyżej trudności w fizycznym lokalizowaniu danych, sam adres IP opatrujący każdy z przetwarzanych w sieciach pakietów danych również nie stanowi jednoznacznego określenia zakończenia sieci, które jest rzeczywistym (fizycznym) źródłem jego pochodzenia. W szczególności, pakiety danych mogą podlegać specyficznemu fałszerstwu zwanemu z ang. *IP spoofing*, polegającemu na wysyłaniu pakietów z przerobionym adresem nadawczym (niczym tradycyjny list fałszywie podpisany w imieniu innej osoby lub wręcz wskazujący nieistniejącego nadawcę). Dane mogą ponadto być także przekierowywane pomiędzy węzłami komunikacyjnymi, komputerami, tak że adresem IP pochodzenia określonej porcji danych jest adres ostatniej maszyny biorącej udział w pośredniczeniu w ruchu (rolę taką pełnią m.in. serwery *proxy*; szczególnym przykładem takiego trasowania ruchu jest także opisywana w rozdziale III. niniejszej pracy sieć TOR, zapewniająca anonimizację ruchu poprzez organizowanie szeregu skoków po losowo wyznaczanych węzłach pośredniczących). Pakiety danych o zmodyfikowanym, czy też ukrytym adresie IP pochodzenia, mogą być namierzane wyłącznie na podstawie analizy tzw. logów sieciowych, czyli dzienników zawierających historię ruchu wybranego fragmentu cyberprzestrzeni.

Logi sieciowe - zapisywane w postaci plików, w tym też plików bazodanowych, to odpowiedniki zestawień połączeń telefonicznych (tzw. billingów), wskazujące zakończenia sieci, identyfikowane poprzez ich adresy IP, biorące udział w określonej wymianie danych. Obok adresów nadawcy oraz odbiorcy woluminu danych, logi sieciowe wskazują także na czas występowania ruchu oraz jego ewentualne przerwy. Logi nie zawierają kopii samych przekazywanych danych (analogicznie, jak bilingi telefoniczne) choć w wielu przypadkach zdradzają, jakie dane - to jest o jakiej zawartości, były przedmiotem transmisji, np. analiza ruchu sieciowego określonej strony internetowej, na której bezpośrednio dostępne są nielegalne treści (tzn. wyświetlają się na stronie już bez konieczności podejmowania jakichkolwiek działań przez użytkownika), wskazuje jakie adresy IP pobierały te treści. Kwestia ta, będąca zarzewiem wielu dyskusji problematyki retencji danych, powoduje specyficzne zacieranie się granic pomiędzy pozyskiwaniem wyłącznie danych o ruchu, a pozyskiwaniem zawartości przekazu (dokonywanego z zachowaniem dużo ostrzejszych rygorów prawnych) w obszarze cyberprzestrzeni. O ile z technicznego punktu widzenia każdy użytkownik sieci może gromadzić logi ruchu wykonywanego z udziałem jego komputera, czy też sieci lokalnej (np. ruchu na routerze bezprzewodowym), o tyle z punktu widzenia prawnego do gromadzenia historii ruchu sieciowego zobowiązani są wyłącznie tzw. przedsiębiorcy telekomunikacyjni, będący operatorami (dostarczycielami sieci) lub dostawcami usług telekomunikacyjnych. Obowiązek ten, stanowiący element tzw. retencji danych - czyli regulacji nakazujących przedsiębiorcom telekomunikacyjnym przetrzymywanie określonych danych o obsługiwanym ruchu (bez samej „zawartości" ruchu) został uregulowany w polskim prawie w przepisach ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne[29]. Zgodnie z przepisem art. 180a ustawy:

„Art. 180a.

1. Z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt:

1) zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi;

[29] Dz. U. Nr 171, poz. 1800.

2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom, a także Służbie Celnej, sądowi i prokuratorowi, na zasadach i w trybie określonych w przepisach odrębnych;

3) chronić dane, o których mowa w pkt 1, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami art. 159–175a, art. 175c i art. 180e.”

Uzupełniające, zgodnie z przywołanym w powyższym artykule przepisem art. 180c, obowiązkiem retencji danych objęte są dane niezbędne do:

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:
    a) inicjującego połączenie,
    b) do którego kierowane jest połączenie;
2) określenia:
    a) daty i godziny połączenia oraz czasu jego trwania,
    b) rodzaju połączenia,
    c) lokalizacji telekomunikacyjnego urządzenia końcowego.

W konsekwencji, należy zaznaczyć iż zgodnie z polskim ustawodawstwem, na przedsiębiorcach telekomunikacyjnych świadczących publicznie dostępne usługi telekomunikacyjne ciąży obowiązek gromadzenia danych pozwalających na odtworzenie historii ruchu sieciowego, poddającego się identyfikacji poprzez wskazanie dwóch konkretnych, fizycznych zakończeń sieci - to jest nadawcy oraz końcowego odbiorcy, biorących udział w transmisji danych.

Szczegółowy, *stricte* techniczny, katalog danych o ruchu sieciowym, które objęte są powyższym obowiązkiem retencji danych, określony został w akcie wykonawczym wydanym na podstawie art. 180c ust. 2 ustawy - Prawo telekomunikacyjne. Zgodnie z przywołanym aktem, w przypadku identyfikacji użytkowników usług dostępu do Internetu (w odróżnieniu od pozostałych usług telekomunikacyjnych, np. łączności głosowej naziemnej, czy też komórkowej), podstawową daną *teleinformatyczną* (to jest o charakterze technicznym) pozwalającą na identyfikację oraz lokalizację zakończeń transmisji jest opisany wyżej adres IP. Ponieważ pojedynczy adres IP może w jednym czasie być przypisany wyłącznie do jednego - w skali globalnej, fizycznego zakończenia sieci, ustalenie tego adresu pozwala na jednoznaczne wskazanie dwóch systemów (zlokalizowanych do miasta, ulicy, numeru domu

oraz mieszkania), pomiędzy którymi wykonywany był ruch sieciowy. Elementem logów operatorów jest bowiem także prowadzenie spisów korelacji poszczególnych zakończeń sieci, z przypisanymi im adresami IP w ujęciu czasowym. Mając powyższe na uwadze, konieczne jest jednak przypomnienie wcześniejszej uwagi o charakterze merytorycznym, iż zidentyfikowane w opisany sposób zakończenia sieci nie muszą ujawniać rzeczywistych, krańcowych zakończeń nadawcy oraz odbiorcy, bowiem analizowany ruch może być przekierowywany przez dodatkowe maszyny (często w sposób nieuświadamiany przez ich prawnych użytkowników) celem jego anonimizacji. Prowadzenie dalszych ustaleń w przypadku wystąpienia takiej sytuacji wymaga żmudnej analizy danych o ruchu sieciowym, polegającej na korelacji ruchu wchodzącego oraz wychodzącego z danego zakończenia sieci - działanie takie pozwala ustalić, że określony „wychodzący dalej" pakiet danych uprzednio „wpłynął" do systemu działającego pod danym adresem IP z maszyny o innym adresie, lokalizowanym nawet na terytorium innego państwa.

Co istotne, wskazane działania, z uwagi na transgraniczny charakter ruchu sieciowego, mogą wymagać - i w praktyce sytuacja taka zdarza się nagminnie, współpracy organów ścigania z wieloma operatorami telekomunikacyjnymi świadczącymi dodatkowo usługi w różnych krajach. Rzadkością jest bowiem, aby transmisja sieciowa w całości (to jest od „prawdziwego" nadawcy aż do końcowego adresata) zamykała się w infrastrukturze sieciowej jednego dostawcy łącz. Warto również przypomnieć, iż przeprowadzona identyfikacja zakończenia sieci oraz jego właściciela (wykonana np. w oparciu o dane osobowe usługobiorców, przetwarzane przez operatorów telekomunikacyjnych oraz dostawców usług) nie może być zrównywana z ustaleniem sprawcy ewentualnego cyberataku przeprowadzonego z tego zakończenia sieci. Adres IP nie wskazuje bowiem osoby sprawcy, lecz samo miejsce jego działania - lub też miejsce, przez które sprawca ataku przekazywał dalej ruch celem ukrycia jego prawdziwego źródła pochodzenia. Za niedopuszczalne należy uznawać wszelkie próby automatycznego, domyślnego przypisywania winy za atak właścicielowi (dzierżawcy) danego łącza, z którego atak ten został wyprowadzony (winy nie ponosi przecież ani łącze, ani komputer, zaś wobec osób funkcjonuje konstytucyjnie usankcjonowane domniemanie niewinności). Ustalenie miejsca stanowi bowiem wyłącznie punkt wyjściowy do prowadzenia dalszych poszukiwań narzędzia zbrodni, jakim w tym wypadku jest określony system teleinformatyczny - najczęściej standardowy komputer. Dopiero powiązanie tak ustalonego systemu, osoby jego właściciela / użytkownika oraz zakończenia fizycznego sieci pozwalają na rzetelne przeprowadzenie oceny możliwości przypisania winy dokonania ataku określonej osobie, użytkownikowi cyberprzestrzeni.

Obok logów gromadzonych obligatoryjnie przez przedsiębiorców telekomunikacyjnych w ramach procesu retencji danych, potencjalnym źródłem informacji na temat ruchu sieciowego oraz jego przepływów mogą być także logi zbierane dobrowolnie przez osoby fizyczne, czy podmioty nie objęte regulacjami prawnymi w tym zakresie. Przykładowo, większość użytkowników cyberprzestrzeni posiada obecnie zainstalowane na komputerach oprogramowanie antywirusowe[30] oraz tzw. zapory ogniowe, czy też sieciowe[31]. Coraz częściej funkcjonalności takiego oprogramowania włączane są wręcz do podstawowych funkcjonalności nowoczesnych systemów operacyjnych. Elementem pracy tego typu rozwiązań programowych, jak również sprzętowo - programowych zaimplementowanych np. w routerach sieci bezprzewodowych Wi-Fi, jest prowadzenie lokalnych logów ruchu wchodzącego oraz wychodzącego. Z punktu widzenia technicznego, logi takie - choć zbierane zupełnie samodzielnie oraz dobrowolnie przez pojedynczych użytkowników, stanowią istotne źródło wiedzy obrazującej przeprowadzony atak, czy samą jego próbę. Z punktu widzenia procesowego, o ile wykorzystanie takiego materiału jest oczywiście możliwe w ramach realizacji zasady swobodnej oceny dowodów, o tyle jego wiarygodność może być łatwo podważona. Logi zbierane przez oprogramowanie zapisywane są do plików oraz następnie cały czas uzupełniane w drodze tzw. nadpisywania pliku. W konsekwencji, plik logu poddawany jest ustawicznym modyfikacjom, których charakteru nie można jednoznacznie ustalić *ex post*. Innymi słowy, zapisana w metadanych pliku data jego ostatniej modyfikacji może bowiem być zarówno datą jego nadpisania w ramach aktualizacji logu, jak również datą jego nieuprawnionej modyfikacji dokonanej ręcznie przez właściciela systemu, ale także samego włamywacza, zacierającego ślady swojego działania. Celem uniknięcia takich zarzutów, w przypadku logów zbieranych przez przedsiębiorców telekomunikacyjnych, wykorzystywane przez nich w tym celu systemy podlegają szczególnym reżimom ochrony, zarówno w sferze technicznej (specjalne urządzenia brzegowe, oprogramowanie ochronne, zapewnienie bezpieczeństwa kopii zapasowych logów na wypadek ich uszkodzenia), jak i organizacyjnej (procedury przyznawania dostępu do pomieszczeń serwerowni dla personelu, procedury odtwarzania logów, procedury ich ochrony fizycznej, procedury bezpiecznej wymiany urządzeń). Z uwagi na powyższe, tzw. logi

[30] Oprogramowanie chroniące system teleinformatyczny przed jego zainfekowaniem wszelkimi kategoriami oprogramowania złośliwego. Do najpopularniejszych programów antywirusowych zalicza się pakiet *Norton, Kaspersky*, czy *Avast*. Więcej o oprogramowaniu antywirusowym na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Antivirus_software.

[31] Z ang. *firewall*. Oprogramowanie mające na celu blokowanie określonych kategorii ruchu sieciowego wchodzącego oraz wychodzącego. Więcej na temat zasad oraz dokładnych funkcji oprogramowania na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/Zapora_sieciowa.

prywatne, przede wszystkim mogą stanowić wartościowy materiał pomocniczy, pozwalający na przeprowadzenie właściwej oceny dowodowej całokształtu materiału zebranego w sprawie w całym obszarze cyberprzestrzeni.

3. Korelacja dowodowych czynności procesowych podejmowanych w cyberprzestrzeni z czynnościami podejmowanymi poza domeną cyfrową

Powyższa uwaga, kończąca poprzedni punkt rozdziału pozwala na płynne przejście do kolejnego zagadnienia, którym zgodnie z przyjętą konstrukcją pracy jest przybliżenie stosunku, jaki zachodzi pomiędzy źródłami dowodowymi lokowanymi wewnątrz cyberprzestrzeni - a więc dowodami elektronicznymi, a źródłami dowodowymi „zewnętrznymi" (w pewnym uproszczeniu można powiedzieć - klasycznymi) odnoszącymi się wprawdzie do dowodów popełnienia cyberprzestępstwa, jednak nie przybierających *zdematerializowanej* postaci cyfrowej. Do drugiej z wymienionych kategorii dowodowych zaliczyć można przykładowo opinię biegłego, czy też dowód z przesłuchania świadka-funkcjonariusza dokonującego czynności dochodzeniowo - śledczej lub operacyjno - rozpoznawczej w cyberprzestrzeni. Dowód taki - choć posiadający charakter pośredni, to jest nie powstały w czasie samego popełnienia przestępstwa, pozwala z zachowaniem określonych rygorów procesowych na odtworzenie określonego stanu faktycznego (np. zeznanie świadka o wystąpieniu nielegalnych treści na stronie internetowej dostępnej pod określonym adresem WWW)[32].

Z uwagi na coraz wyższy stopień specjalizacji technologii informacyjnych (w tym także stosowanie oprogramowania służącego do anonimizacji danych, czy wręcz ukrywania przez cyberprzestępców śladów zbrodni w drodze stosowania rozwiązań kryptograficznych) - wprowadzenie do postępowania karnego, prowadzonego przecież przez zawodowych prawników, „surowego" dowodu elektronicznego, nie stanowi jednoznacznie o możliwości dokonania przez skład orzekający sądu pełnej oraz rzetelnej oceny stanu faktycznego zaistniałego w danej sprawie w cyberprzestrzeni. Niezbędna wydaje się tu znajomość choćby podstawowych informacji z zakresu funkcjonowania technologii informacyjnych oraz komputerowych, pozwalająca na podjęcie dyskursu w zakresie ataków przeprowadzanych z adresu IP, np. typu DDOS, z zastosowaniem *ip spoofingu*, czy też tzw. *pingowania*. Nie bez znaczenia pozostaje fakt, iż w ocenie prawnej gromadzonego materiału dowodowego o charakterze technicznym nie pomagają także same specjalistyczne zwroty stosowane przez

---

[32] A. Taracha, Czynności operacyjno rozpoznawcze, aspekty kryminalistyczne i prawnodowodowe, Wydawnictwo UMCS, Lublin 2006, s. 221 i nast.

przedstawicieli branży IT, często wręcz niepozwalające na poprawne zrozumienie przez sąd rzeczywistego charakteru opisywanej czynności. Czy bowiem „skanowanie portów" jest już ingerencją w prywatność użytkownika systemu teleinformatycznego? (na marginesie - wydaje się, że nie, bowiem co do zasady stanowi otwartą, dostępna dla wszystkich użytkowników funkcjonalność każdej sieci).

Obok powyższych problemów związanych ze specjalizacją w dziedzinie technologii cyberprzestrzeni, należy również mieć na uwadze sygnalizowane wcześniej trudności w procesowym pozyskiwaniu dowodów elektronicznych, przetwarzanych nierzadko transgranicznie, czy wręcz transkontynentalnie. Coraz częściej zdarza się, iż zdecydowanie szybszym oraz prostszym z punktu widzenia proceduralnego, staje się przyjęcie jako dowodu zeznania osoby ustalającej zaistnienie w sieci określonej okoliczności (np. zeznanie funkcjonariusza policji pełniącego służbę w tzw. *cyberpatrolu*[33]), niż pozyskanie wszystkich logów od operatorów telekomunikacyjnych biorących udział w obsłudze danego przesyłu danych w cyberprzestrzeni oraz zabezpieczenie dowodów elektronicznych. Działanie takie, trzeba jednak mieć na uwadze, iż pomimo swoich zalet w zakresie ekonomiki procesowej, uderza w procesową dyrektywę dążenia sądu do bezpośredniego poznawania materiału dowodowego, pozwalającą nie tylko na urzeczywistnienie zasady sądowej, swobodnej oceny dowodów, ale także stanowiącą gwarancję realnej kontroli funkcjonowania organów ścigania[34].

Powyższe uwagi powodują, iż pomiędzy dowodami elektronicznymi, a dowodami klasycznymi odnoszącymi się do zdarzeń zaistniałych w obszarze cyberprzestrzeni, mogą zachodzić w szczególności dwie następujące zależności:

1) dowody elektroniczne oraz dowody klasyczne mogą się uzupełniać, wspólnie tworząc jednoznaczny obraz stanu faktycznego sprawy (np. opinia biegłego pozwalająca na poprawną ocenę prawną zaistniałych wydarzeń); oraz,
2) dowody klasyczne mogą być stosowane, jako swoisty substytut dowodów elektronicznych, odnosząc się do zdarzeń zaistniałych w domenie cyfrowej, pomimo iż miejscem ich przeprowadzenia nie jest obszar cyberprzestrzeni.

Analizując wskazane konfiguracje dowodowe pod kątem potencjalnego krzyżowania się treści dowodów elektronicznych oraz klasycznych, należy zaznaczyć, iż wyłącznie pierwsze, niejako konkurencyjne, zestawienie różnych form dowodowych w danej sprawie pozwala na

[33] Patrole takie przeczesują sieć w poszukiwaniu materiałów nielegalnych, np. pornografii z udziałem dzieci.
[34] Dyrektywy analizowane szeroko przez A. Gaberle, op. cit., s. 23 i nast.

zebranie pełnego - a w konsekwencji także rzetelnego, materiału dowodowego realizującego zasady procesu karnego, w tym zasadę *in dubio pro reo*[35]. W sytuacji bowiem, gdy dowody różnych rodzajów tworzą spójny obraz *modus operandi* sprawcy cyberataku, popierając tym samym jednakową hipotezę przebiegu wydarzeń, dowody te wzmacniają swoją moc na zasadzie synergii. W sytuacji zaś, gdy np. opinia biegłego podważa wartość dowodu elektronicznego (np. opinia potwierdzająca fałszerstwo zapisów o ruchu sieciowym zgromadzonych w logach sieciowych, czy też opinia wskazująca na nieświadomy udział domniemanego sprawcy, który zwyczajnie padł ofiarą oprogramowania złośliwego przejmującego kontrolę nad zainfekowanym systemem), należy mówić nie tyle o wspomagającej, co wręcz kontrolnej roli dowodów klasycznych wobec dowodów elektronicznych - w istocie tworzonych w zautomatyzowanych układach systemów teleinformatycznych oraz urządzeniach komutacyjnych nowoczesnych sieci telekomunikacyjnych budujących podwaliny cyberprzestrzeni.

4. Kwestia dopuszczalnego prawnie zasięgu realizacji czynności procesowych podejmowanych w obszarze cyberprzestrzeni

Funkcjonujący obecnie w krajowym porządku prawnym brak regulacji prawnych odnoszących się *expressis verbis* do specyfiki podejmowania czynności procesowych w cyberprzestrzeni w żadnym razie nie może być odczytywany, jako oznaczający wyłączenie tych czynności z zakresu działania jakichkolwiek przepisów[36] gwarantujących ochronę podstawowych praw człowieka i obywatela - w tym ochronę przed bezprawnym działaniem instytucji państwowych, przewidzianą tak w przepisach Kodeksu postępowania karnego, innych ustaw, jak i Konstytucji RP oraz wiążących Polskę umów międzynarodowych. Z punktu widzenia prawnego, w szczególności nie jest możliwe uznanie cyberprzestrzeni za obszar, w którym organy państwa - a w tym organy ścigania, miałyby działać w sposób nieskrępowany, podejmując czynności wyłącznie wedle własnego uznania, czy też choćby swobodniej niż ma to miejsce w przypadku czynności konwencjonalnych, podejmowanych w rzeczywistości *fizycznej*.

Zarysowana powyżej problematyka zakresu działalności podmiotów państwowych

[35] Konkurencja materiału dowodowego stanowi m. in. gwarancję obiektywizmu postępowania, nakazującego rozpatrywanie każdego dowodu w sposób niezmierzający do zastosowania go jako narzędzia do potwierdzenia z góry założonej już tezy. Więcej na ten temat: A. Tęcz-Paciorek, Zasada domniemania niewinności w polskim procesie karnym, Lex, Warszawa 2012, s. 136-138.

[36] J. L. Goldsmith, *Against Cyberanarchy, University of Chicago Law* Review *Fall 1998*, Chicago 1998. Opracowanie dostępne na stronie internetowej pod adresem: http://cyber.law.harvard.edu/property00/jurisdiction/cyberanarchy.html.

nabiera szczególnego znaczenia w obszarze cyberprzestrzeni z uwagi na cyfrową, nienamacalną strukturę przestrzeni definiowanej tym wyrażeniem. Cyberprzestrzeń, będąca obszarem wyłącznie logicznym - to jest obszarem, w którym nie obowiązują zasady odnoszące się do topologii przestrzeni fizycznej, umożliwia bowiem znacznie szerszy zakres ingerencji służb państwowych w życie obywatela-użytkownika domeny cyfrowej, niż ma to miejsce w przypadku działania tychże podmiotów w otaczającej rzeczywistości. Nie tylko bowiem działania podejmowane w cyberprzestrzeni nie są ograniczane przez wymiary odnoszące się do określania *odległości*, ale co więcej - omijają wszelkie zabezpieczenia fizyczne, jak choćby drzwi domu, czy otaczające go ogrodzenia, pozwalając jednocześnie na prowadzenie czynności w sposób niewyrządzający szkód fizycznych, ale także wręcz utajniony przed oczami adresata czynności. Z punktu widzenia technicznego nie ma bowiem istotnych ograniczeń w możliwości np. prowadzenia przeszukania zawartości systemu teleinformatycznego za pośrednictwem cyberprzestrzeni, to jest *on-line*, bez jakiejkolwiek ingerencji fizycznej w złącza danego komputera lub jego informatycznych nośników danych. Przeszukanie takie nie będzie wymagało fizycznego dostępu do systemu, w szczególności zaś nie będzie wymagało jego wydania celem dokonania czynności procesowego zabezpieczenia, zaś uzyskane w ten sposób materiały dowodowe będą idealną kopią plików pierwotnych.

Sygnalizowana kwestia podejmowania czynności procesowych w cyberprzestrzeni „na odległość" od lat stanowi przedmiot licznych kontrowersji[37], nie znajdując jakichkolwiek rozwiązań prawnych. Warto zaznaczyć, iż sam pomysł uzyskiwania przez służby państwowe dostępu do komputerów obywateli za pośrednictwem cyberprzestrzeni - niosący potencjalne zagrożenie masowej wręcz inwigilacji społeczeństwa, doprowadził do wybuchu przynajmniej kilku afer międzynarodowych, w tym między innymi zdarzeń mających miejsce w 2014 r., stawiających pod znakiem zapytania poczynania rządu USA, który za pośrednictwem Narodowej Agencji Bezpieczeństwa (*National Security Agency* - w skrócie NSA) miał inwigilować nie tylko obywateli swojego kraju, ale także użytkowników wielu usług sieciowych z całego świata (np. poczty Google Mail - Gmail, poczty Yahoo, czy też portalu społecznościowego Facebook)[38] celem zwalczania oraz zapobiegania zagrożeniom o charakterze terrorystycznym. Nie mniejszą debatę w odniesieniu do kwestii zdalnego uzyskiwania dostępu do komputerów przez wybrane służby państwowe wywołały także

[37] Problematykę tę zaznacza także A. Lach w: Dowody cyfrowe..., op. cit., s. 3-4 oraz A. Adamski w: Przestępczość w cyberprzestrzeni..., op. cit., s. 129.

[38] Afera dotyczyła ujawnianie funkcjonowania tzw. systemu PRISM. Więcej na jego temat znaleźć można na licznych stronach internetowych poświęconych tematyce budowy oraz działania PRISM, jak np. na stronie internetowej dostępnej pod adresem http://pl.wikipedia.org/wiki/PRISM_(program_szpiegowski).

doniesienia o przygotowaniu przez administrację Niemiecką w 2011 r. tzw. rządowego trojana[39] (*Bundestrojaner*, czy też *Staatstrojaner*), stanowiącego stworzone na zamówienie państwa oprogramowanie złośliwe pozwalające na potajemne włamywanie się do komputerów obywateli celem prowadzenia kontroli ich ruchu sieciowego, w tym przechwytywanie elektronicznej korespondencji oraz innych komunikatów nadawanych przez sieć, jeszcze przed ich wysłaniem z komputera (kwestia ta ma istotne znaczenie np. z punktu widzenia przechwytywania wiadomości szyfrowanych jeszcze przed ich zabezpieczeniem, gdy wciąż pozostają zapisane tzw. otwartym tekstem). W obydwu przypadkach wskazywane działania państw prowadzone były bez jednoznacznych podstaw prawnych, zaś ich obnażenie miało miejsce na wskutek działania osób trzecich. Znamiennym stało się, że wykrycie niemieckiego programu szpiegującego zostało dokonane przez grupę hackerską CCC (*Chaos Computer Club*), która w przy okazji swoich bezprawnych działań dostrzegła pojawianie się na komputerach ofiar swoich ataków oprogramowania wykonującego niejasne operacje sieciowe. Analiza kodu źródłowego rzeczonego oprogramowania pozwoliła na ustalenie jego powiązania z firmą realizującą kontrakt rządowy na oprogramowanie mające być wykorzystywane przez niemiecką policję kryminalną.

Jak zostało zauważone na wstępie niniejszego punktu rozdziału, obowiązujący w Polsce porządek prawny nie zawiera regulacji odnoszących się specyficznie do podejmowania czynności *wewnątrz* cyberprzestrzeni (czynnością taką w żadnym razie nie jest fizyczne zabezpieczenie komputera, czy też nośnika, dokonywane w całości *poza* obszarem cyberprzestrzeni). Tym samym, w zakresie faktycznego podejmowania takich czynności, niezbędne staje się odpowiednie stosowanie regulacji o charakterze ogólnym, odnoszących się czy to do zasad prowadzenia poszczególnych czynności procesowych, czy też zawierających podstawy prawne do podejmowania określonych działań przez organy wymiaru sprawiedliwości. W szczególności, karnoprocesowym przykładem regulacji nakazującej stosowanie takiej analogii jest przepis art. 236a Kodeksu postępowania karnego[40], w brzmieniu:

„Art. 236a.

Przepisy rozdziału niniejszego stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu

[39] Nieco więcej na temat oprogramowania m.in. na stronie Internetowej dostępnej pod adresem: http://de.wikipedia.org/wiki/Online-Durchsuchung.

[40] Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego, Dz. U. Nr 89 poz. 555, z późn. zm. Pełny tekst ustawy dostępny na stronie internetowej pod adresem: http://isap.sejm.gov.pl/DetailsServlet?id=WDU19970890555

informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną.”

Rzeczona analogia - z uwagi na szczególny charakter cyberprzestrzeni, staje się jednak nierzadko trudna do zastosowania w praktyce, nastręczając licznych trudności oraz pytań odnośnie przeprowadzenia procesowej oceny określonej czynności faktycznej podejmowanej w ramach postępowania o przestępstwo popełnione w cyberprzestrzeni. Sztandarowym przykładem przywoływanych trudności jest kwestia procesowego zabezpieczania za pośrednictwem cyberprzestrzeni - a zatem wyłącznie w sieci, nielegalnych treści pojawiających się na stronach internetowych, których pliki alokowane są fizycznie na serwerach rozrzuconych po całym świecie. W zarysowującej się praktyce, sądy podchodzą niezwykle ostrożnie do kwestii przyjmowania za dowód w rozumieniu procesowym kopii strony (tzw. zrzutu) wykonanej przez funkcjonariusza np. Policji przy użyciu komputera działającego na posterunku, wymagając aby materiał taki, jedynie wsparty stosowną notatką urzędową (zgodnie z zakazem dowodowym zawartym w przepisie art. 174 Kodeksu postępowania karnego), został przetransponowany do procesu karnego w postaci zeznania świadka-funkcjonariusza. W zeznaniu takim przywołany zostaje przykładowo adres strony WWW, na której możliwe do znalezienia były określone treści nielegalne, odpowiadający wskazanej domenie adres IP strony zgodny z tablicą DNS oraz dane dot. podmiotu rejestrującego domenę - ustalone choćby na podstawie ogólnie dostępnej usługi sieciowej WHOIS. Należy zaznaczyć, iż bezbłędne przywołanie przez funkcjonariusza przytoczonych danych wyłącznie z pamięci w ramach składanego zeznania wydaje się mało prawdopodobne, gdy sam adres IP może składać się nawet z kilkunastu cyfr, zaś nazwa domeny oraz szczegółowy adres strony mogą stanowić ciąg nawet kilkudziesięciu i więcej znaków, które nie muszą wcale składać się na zrozumiałe dla człowieka wyrazy. Wydaje się, iż w takich sytuacjach zastępowanie łatwo dostępnego dowodu elektronicznego znaną już formą zeznania świadka stanowi swoiste trywializowanie problematyki przestępczości cybernetycznej. W związku z powyższym, za istotną słabość legislacyjną polskiego prawa należy uznawać brak jakichkolwiek regulacji, określających choćby zasady podejmowania czynności procesowych w specyficznym obszarze domeny cyfrowej. Z uwagi na ogólny charakter niniejszej części rozdziału, szczegółowe rozważania na temat oceny prawnej prowadzenia podsłuchu procesowego w sieci oraz realizacji tzw. przeszukań *on-line* (sygnalizowanych nieco wyżej) zostały zawarte w części kolejnej - zgodnie z przyjętą na wstępie budową rozdziału.

Przedstawiając własny głos w ogólnej debacie na temat dopuszczalności prowadzenia czynności procesowych za pośrednictwem cyberprzestrzeni (choć problematykę tę warto rozszerzyć także na obszar realizacji czynności operacyjno-rozpoznawczych), należy zaznaczyć, iż czynności takie niosą ze sobą wiele wyzwań prawnych oraz równie dużo usprawnień w pracy organów ścigania, co zagrożeń dopuszczania się nadużyć o potencjalnie globalnej skali - to jest skali cyberprzestrzeni. Do najważniejszych „za i przeciw" podejmowania czynności procesowych za pośrednictwem cyberprzestrzeni zaliczyć należy w szczególności:

- istotne ułatwienia w faktycznym realizowaniu uprawnień procesowych przez organy ścigania, z jednoczesnym zagwarantowaniem zachowania jakości pozyskiwanego materiału dowodowego (pliki zgrane przez sieć stanowią co do zasady idealną kopię materiału źródłowego),
- możliwość pominięcia wielu utrudnień związanych z koniecznością korzystania z pomocy prawnej celem fizycznego zabezpieczenia zagranicznego serwera WWW, na którym *hostowana* (utrzymywana, obsługiwana) jest określona strona WWW, czy też usługa sieciowa (warto zaznaczyć, iż strona taka lub usługa mogą być własnością polaka, którego działalność kierowana jest wyłącznie do odbiorców polskich, co w żadnej mierze nie przeszkadza aby stosowne pliki znajdowały się na komputerze np. na Filipinach, zaś odnośny ruch sieciowy był przekazywany przez kilka krajów ze wszystkich kontynentów),
- możliwość szerokiego stosowania dowodów elektronicznych, zdobywanych w ramach prostego zabezpieczenia dokonywanego przez odpowiednio przeszkolonego funkcjonariusza, wykorzystującego oprogramowanie zapewniające integralność plików zabezpieczonych *on-line* (zabezpieczenie takie zapewni niepodważalność dowodu poprzez wykluczenie możliwości jego późniejszej modyfikacji - co z punktu widzenia technicznego jest niestety niezwykle proste),
- przyspieszenie reakcji organów ścigania pozyskujących informację o popełnieniu przestępstwa, mogących np. dokonać zatrzymania funkcjonowanie systemu służącego do przeprowadzenia aktualnie toczącego się ataku cybernetycznego,
- z uwagi na cyfrową formę zapisu dowodów elektronicznych ich integralność (*oryginalność*) zawsze poddawana jest większym zastrzeżeniom, niż ma to miejsce w przypadku dowodów fizycznych. Pozyskiwanie dowodów za pośrednictwem cyberprzestrzeni w pewnej mierze może być odbierane, jako podważające wartość

materiału dowodowego, który mógł ulec nieautoryzowanym lub choćby przypadkowym (np. spowodowanym błędami w łączności) modyfikacjom w trakcie prowadzenia czynności zabezpieczenia (*vide* jednak uwagi do kolejnego punktu I.5 rozdziału),

- jakakolwiek ingerencja w systemy osób fizycznych bezwzględnie zawsze rzucać będzie cień co do szczegółowych okoliczności prowadzenia czynności procesowych dokonywanych *on-line*. Skoro bowiem określony podmiot uprawniony do realizacji czynności uzyskał dostęp do systemu teleinformatycznego obywatel - mógł on przecież nie tylko doprowadzić do zgrania z tego systemu określonych plików, ale także ich uprzedniego, oczywiście bezprawnego umieszczenia tam celem podrzucenia dowodu,
- od początku debacie na temat prowadzenia czynności procesowych za pośrednictwem sieci towarzyszy debata na temat granic ingerencji służb państwowych w życie prywatne obywateli, wskazująca na ryzyka związanie z faktycznymi możliwościami prowadzenia globalnej inwigilacji przez podmioty mogące legalnie podejmować określone czynności w domenie cyberprzestrzeni.

Ostatecznie, warto również wskazać, iż w świetle obowiązującego prawa krajowego, jedyną regulacją prawną - jednak nie posiadającą charakteru karnoprocesowego, odnoszącą się do kwestii dopuszczalnego prawnie zakresu bezpośredniego ingerowania w system teleinformatyczny użytkownika końcowego, jest norma zawarta w art. 173 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne[41]. Zasadniczym celem wprowadzenia przywołanego przepisu stało się uregulowanie kwestii wykorzystywania przez operatorów oraz dostawców usług sieciowych, a także podmioty świadczące usługi drogą elektroniczną, technologii internetowej tzw. plików ciasteczek (z ang. *cookies*) pozwalających na tymczasowe zapisywanie na komputerze użytkownika końcowego określonych informacji, służących bezpośrednio do realizacji świadczonych usług (np. zapisania faktu otwarcia tzw. sesji, dzięki czemu przy nawigowaniu przez kolejne podstrony określonego portalu nie jest konieczne ustawiczne powtarzanie procesu logowania oraz podawania hasła). Poniżej brzmienie przywołanego przepisu:

„Art. 173.

1. Przechowywanie informacji lub uzyskiwanie dostępu do informacji już

[41] Dz. U. Nr 171, poz. 1800, wraz z późn. zm. Pełny tekst ustawy dostępny na stronie internetowej pod adresem: http://isap.sejm.gov.pl/DetailsServlet?id=WDU20041711800.

przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego jest dozwolone, pod warunkiem że:

1) abonent lub użytkownik końcowy zostanie uprzednio bezpośrednio poinformowany w sposób jednoznaczny, łatwy i zrozumiały, o:

a) celu przechowywania i uzyskiwania dostępu do tej informacji,

b) możliwości określenia przez niego warunków przechowywania lub uzyskiwania dostępu do tej informacji za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi;

2) abonent lub użytkownik końcowy, po otrzymaniu informacji, o których mowa w pkt 1, wyrazi na to zgodę;

3) przechowywana informacja lub uzyskiwanie do niej dostępu nie powoduje zmian konfiguracyjnych w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego i oprogramowaniu zainstalowanym w tym urządzeniu.

2. Abonent lub użytkownik końcowy może wyrazić zgodę, o której mowa w ust. 1 pkt 2, za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi.

3. Warunków, o których mowa w ust. 1, nie stosuje się, jeżeli przechowywanie lub uzyskanie dostępu do informacji, o której mowa w ust. 1, jest konieczne do:

1) wykonania transmisji komunikatu za pośrednictwem publicznej sieci telekomunikacyjnej;

2) dostarczania usługi telekomunikacyjnej lub usługi świadczonej drogą elektroniczną, żądanej przez abonenta lub użytkownika końcowego.

4. Podmioty świadczące usługi telekomunikacyjne lub usługi drogą elektroniczną mogą instalować oprogramowanie w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego przeznaczonym do korzystania z tych usług lub korzystać z tego oprogramowania, pod warunkiem że abonent lub użytkownik końcowy:

1) przed instalacją oprogramowania zostanie poinformowany bezpośrednio, w sposób jednoznaczny, łatwy i zrozumiały, o celu, w jakim zostanie zainstalowane oprogramowanie, oraz sposobach korzystania przez podmiot świadczący usługi z tego oprogramowania;

2) zostanie poinformowany bezpośrednio, w sposób jednoznaczny, łatwy i zrozumiały, o sposobie usunięcia oprogramowania z telekomunikacyjnego urządzenia końcowego użytkownika lub abonenta;

3) przed instalacją oprogramowania wyrazi zgodę na jego instalację i używanie."

Co istotne, powyższa regulacja nie tylko wprowadza obowiązek informowania użytkownika o fakcie wykorzystywania w danej usłudze sieciowej funkcjonalności zapisywania na jego systemie określonych treści, ale także wprost wymaga aby działanie takie zostało autoryzowane uprzednią zgodą - która uwzględniając specyfikę działania cyberprzestrzeni, może jednak zostać wyrażona w sposób dorozumiany, poprzez odpowiednie ustawienia konfiguracyjne systemu użytkownika.

5. Kwestia bezstratnej duplikacji dowodów elektronicznych z punktu widzenia procesowego

W ramach uwag ogólnych dotyczących podejmowania czynności procesowych wewnątrz obszaru cyberprzestrzeni, na osobną analizę zasługuje także kwestia karnoprocesowej oceny możliwości bezstratnego powielania dowodów elektronicznych, występujących przecież nie w formie namacalnej (*vide* wcześniejsze uwagi na temat dowodów elektronicznych zawarte w rozdziale VI pracy) lecz jako cyfrowy zapis. Co było sygnalizowane już wcześniej, zapis taki z punktu widzenia technicznego może być powielany (kopiowany) bez najmniejszych strat lub zmian, pozwalając na wytworzenie potencjalnie nieskończonej liczby egzemplarzy danego dowodu. Wykonana kopia pliku bądź jego części (w istocie dowolnej porcji danych komputerowych zapisanych w formie bitów) nie pozwala na odróżnienie materiału oryginalnego od powielonego.

Celem praktycznego zapewnienia pełnej identyczności powielanych plików niezbędne jest jednak aby w trakcie ich kopiowania stosowane były specjalistyczne narzędzia teleinformatyczne, pozwalające na ominięcie określonych funkcjonalności systemów operacyjnych - w szczególności zaś funkcjonalności dopisujących do każdego pliku tzw. metadane[42], zawierające np. informację o tym kiedy plik został utworzony, otwarty (użyty w przypadku oprogramowania), czy też zmodyfikowany. Proste skopiowanie pliku z zastosowaniem komend systemowych (czy też jego tzw. przeniesienie pomiędzy otwartymi oknami nośników) spowoduje bowiem zmianę metadanych, co będzie stanowić o zasadności podważenia tak zabezpieczonego dowodu, jako w istocie różnego od oryginału, choć nie

[42] M. Cross, D. Littlejohn Shinder, op. cit., s. 122 i nast. W polskim piśmiennictwie problem zaznacza m.in. J. Błachut, op. cit., s. 126.

w zakresie samej zawartości pliku. Zapewnienie identyczności odbioru kopiowanego materiału dowodowego w postaci elektronicznej może także wymagać zapisania kopii na ściśle określonym urządzeniu, pochodzącym od określonego producenta, bowiem różne kontrolery zapisu i odczytu danych, mogą w różny sposób scalać dane zapisane w postaci tzw. fragmentowanej.

Z uwagi na wskazywane aspekty techniczne opisujące działanie systemów teleinformatycznych, faktyczne zabezpieczanie dowodów elektronicznych nie tylko uzasadnia dokonywanie kopii nośników danych (na których potencjalnie mogą znajdować się dowody) oraz następne poszukiwanie materiałów dowodowych już na samej kopii, ale nierzadko wręcz wymaga skopiowania takiego nośnika celem zapewnienia poprawności zabezpieczenia dowodu elektronicznego o charakterze ulotnym. Za prosty takiego technicznie wymuszonego kopiowania dowodów elektronicznych posłużyć może kwestia pozyskiwania danych przetwarzanych wyłącznie tymczasowo w pamięci operacyjnej komputera (RAM) - a zatem danych przetwarzanych w systemie lecz jeszcze niezapisanych w sposób trwały na dysku twardym lub innym nośniku pamięci (jak choćby dopiero przygotowywana korespondencja elektroniczna, czy też liczne rodzaje danych wpisywanych do programów niezapisujących postępów prac użytkownika, np. komunikatorów internetowych, w których możliwe jest wyłączenie zachowywania historii rozmów). Dane takie po wyłączeniu komputera (obniżeniu napięcia elektrycznego w układzie kości pamięci RAM) ulegają bezpowrotnemu usunięciu. Z uwagi na niemożliwość faktycznego utrzymywania zabezpieczanego systemu teleinformatycznego włączonego ustawicznie do prądu (co wymagałoby stabilnego, nieprzerwanego źródła energii) dowód występujący w chwili jego zabezpieczania wyłącznie w formie, jak opisywana powyżej, może w efekcie zostać zachowany jedynie poprzez dokonanie jego kopii. W innym przypadku - przestanie istnieć. W ujęciu technicznym, za dokonywaniem kopii dowodów elektronicznych przemawia także argument minimalizacji ciężarów, jakie ponieść musi podmiot dysponujący materiałem dowodowym zapisanym na pozostających w jego dyspozycji informatycznych nośnikach danych. Zabezpieczając bowiem nośnik fizycznie (jako rzecz), pozbawia się jego użytkownika faktycznego władztwa nie tylko nad materiałem interesującym organy ścigania, ale także wszelkim innym zapisanym w obszarze jego pamięci. Ponadto, w przypadku stosowania tzw. macierzy dyskowych (czyli systemów dysków twardych lub innych informatycznych nośników danych budujących jeden duży bank pamięci), odłączenie nawet tylko jednego dysku może spowodować dysfunkcję

całej macierzy oraz brak dostępu do wszystkich zgromadzonych w niej danych[43]. Potencjalnie, nietrudno ocenić, iż w sytuacji choćby potencjalnej możliwości utraty prowadzenia działalności gospodarczej opierającej się na stosowanych w przedsiębiorstwie rozwiązaniach teleinformatycznych, wielu przedsiębiorców będzie unikać informowania organów ścigania o fakcie posiadania określonych dowodów na swoich firmowych nośnikach danych. Stwierdzenie to dotyczy w ogromnej mierze także podmiotów świadczących usługi informatyczne na rzecz osób trzecich, które wnosząc zawiadomienie o popełnieniu przestępstwa - np. wystąpieniu cyberataku, mogą zostać pozbawione możliwości wywiązania się ze swoich zobowiązań umownych wobec wielu klientów, nie tylko tych objętych danym wydarzeniem, narażając się tym samym na odpowiedzialność cywilną np. z tytułu niedostępności określonych usług gwarantowanych, czy co gorsza - utraty kontroli nad powierzonymi dokumentami zawierającymi informacje o charakterze tajemnicy przedsiębiorcy.

Przenosząc prowadzone rozważania na temat oceny wartości dowodowej kopii dowodów elektronicznych na grunt prawny, należy zauważyć, iż co do zasady, obowiązujące zasady postępowania karnego nie sprzeciwiają się traktowaniu skopiowanego materiału, jako pełnoprawnego dowodu potwierdzającego wystąpienie określonych okoliczności faktycznych. Pomimo występującego na gruncie prawa karnego procesowego braku legalnej definicji pojęcia „dowód", zarówno w doktrynie, jak i ugruntowanym już od lat orzecznictwie, za dowód w ujęciu szerokim uważa się każdy materiał potwierdzający wystąpienie określonych okoliczności faktycznych o charakterze prawnie relewantnym dla prowadzonej sprawy, w tym odnoszących się do oceny winy sprawcy czynu. Stosując w tym miejscu posiłkowo definicję legalną dowodu wprowadzoną w przepisach ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego[44], zgodnie z przepisem art. 227 wskazanej ustawy „Przedmiotem dowodu są fakty mające dla rozstrzygnięcia sprawy istotne znaczenie.". Powyższych rozważań o charakterze generalnym nie sposób nie uzupełnić przywołaniem postanowień art. 170 § 1 Kodeksu postępowania karnego, określającego w sposób negatywny kategorii celowościowych wniosków dowodowych podlegających oddaleniu z mocy ustawy. Zgodnie z obecnym brzmieniem przywołanego przepisu są to:

[43] Sytuacja taka może mieć miejsce np. przy stosowaniu macierzy działających w systemie RAID w opcji maksymalizującej szybkość pracy macierzy, to jest gdy wszystkie dyski zapisują przetwarzane pliki równolegle, ale fragmentarycznie (następuje zsumowanie szybkości zapisu wszystkich dysków).

[44] Dz. U. Nr 43 poz. 296. Pełny tekst ustawy dostępny na stronie internetowej pod adresem: http://isap.sejm.gov.pl/DetailsServlet?id=WDU19640430296.

„Art. 170.

§ 1. Oddala się wniosek dowodowy, jeżeli:

1) przeprowadzenie dowodu jest niedopuszczalne,

2) okoliczność, która ma być udowodniona, nie ma znaczenia dla rozstrzygnięcia sprawy albo jest już udowodniona zgodnie z twierdzeniem wnioskodawcy,

3) dowód jest nieprzydatny do stwierdzenia danej okoliczności,

4) dowodu nie da się przeprowadzić,

5) wniosek dowodowy w sposób oczywisty zmierza do przedłużenia postępowania."

A contrario, wnioski zmierzające do osiągnięcia innych celów niż wskazane w przepisie, są prawnie dopuszczalne, w tym niezależnie od faktu, czy odnoszą się do oryginału, czy też kopii materiału dowodowego występującego w postaci cyfrowego zapisu danych.

Uzupełniająco, w myśl postanowień przepisu art. 170 § 2 Kodeksu postępowania karnego dowód może zmierzać tak do wykazania określonych zdarzeń, jak również obalenia tezy o ich wystąpieniu (w przypadku cyberprzestępczości - np. do wykazania *modus operandi* sprawcy ataku, czy też dowiedzenia, iż brak dostępności serwera spowodowany był wyłącznie samoistnym błędem oprogramowania). Zgodnie z przepisem art. 169 § 2 Kodeksu postępowania karnego, wniosek dowodowy zmierzający do ustalenia określonych okoliczności sprawy może zmierzać także do samego wykrycia lub oceny właściwego dowodu w sprawie.

Odnosząc się do przepisów art. 170 § 1 Kodeksu postępowania karnego, podstawowym warunkiem dla dopuszczalności przyjęcia kopii materiału elektronicznego jako dowodu w procesie, jest spełnienie przez wybrany materiał wszystkich wymogów prawnych związanych z jego pozyskaniem oraz zabezpieczeniem, w szczególności zaś wymogów ustanawiających gwarancje praw człowieka i obywatela oraz zakres zadań i uprawnień poszczególnych organów ścigania podejmujących czynności w cyberprzestrzeni. Pełne zastosowanie znajduje w tym miejscu przepis art. 168a Kodeksu postępowania karnego, który z dniem 1 lipca 2015 r. otrzymuje brzmienie:

„Art. 168a.

Niedopuszczalne jest przeprowadzenie i wykorzystanie dowodu uzyskanego do celów postępowania karnego za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 Kodeksu karnego."

Podkreślenia w tym miejscu wymaga fakt, iż wykonanie - czy to na polecenie sądu, organu

prowadzącego postępowanie przygotowawcze, czy też innego uprawnionego podmiotu - kopii materiału dowodowego występującego w postaci danych elektronicznych, który to materiał został uprzednio pozyskany w sposób niezgodny z prawem, a w szczególności w ramach popełnienia przestępstwa, w żadnej mierze nie może być postrzegane jako uzdrawiające określony dowód poprzez jego pozyskanie (a de facto *wytworzenie*) w ramach dalszych, legalnych już działań. Kopia danych zdobytych w sposób nielegalny musi bowiem dziedziczyć wszystkie cechy formalne oryginalnego materiału, analogicznie, jak przenosi jego pełną zawartość treściową. Innymi słowy - kopia materiału podlegającego wykluczeniu z postępowania karnego z przyczyn prawnych również musi podlegać takiej ocenie.

W kontekście specyfiki zwalczania cyberprzestępczości, szczególnego znaczenia nabierają natomiast postanowienia pkt 2 -5 poruszanego § 1 art. 170 Kodeksu postępowania karnego (wyłączenia wniosków dowodowych z uwagi na: 2) brak znaczenia dowodu dla rozstrzygnięcia sprawy lub potwierdzanie przez dowód faktów bezspornych; 3) nieprzydatność dowodu do stwierdzenia danej okoliczności; 4) niemożliwość przeprowadzenia dowodu; oraz 5) ocenę wniosku, jako w sposób oczywisty zmierzającego do przedłużenia postępowania. Przywołane punkty, odnosząc się do faktycznej oceny materiału dowodowego, który miałby być uzyskany w ramach realizacji danego wniosku, wymagają bowiem specjalistycznej wiedzy w zakresie funkcjonowania systemów teleinformatycznych, sieci komputerowych oraz samego zjawiska cyberprzestępczości. W szczególności, bez choćby podstawowych informacji w zakresie technicznym, nie jest możliwe dokonanie oceny, czy dany wniosek rzeczywiście pozwoli na ustalenie tych okoliczności faktycznych sprawy, które umożliwią przeprowadzenie pełnej oraz rzetelnej rekonstrukcji wydarzeń, a także następcze zweryfikowanie uzyskanych materiałów pod kątem realizacji postawionego celu dowodowego.

Kończąc przedmiotowe rozważania prawne w odniesieniu do dopuszczalności posługiwania się w procesie karnym kopiami dowodów występujących w postaci elektronicznej, warto również nadmienić, iż z uwagi na identyczność kopii materiałów elektronicznych do ich oryginałów, w przypadku prokuratorskiej lub sądowej oceny danych już powielonych, nie należy mówić o jakimkolwiek naruszeniu zasady bezpośredniości zapoznawania się z materiałem dowodowym przez organy procesowe, bowiem kopia zapewnia dokładnie takie same możliwości interakcji procesowej z materiałem jak zapis oryginalny, z którego kopię tę przygotowano. Jedyne w tym względzie ograniczenia o charakterze technicznym, mogą wymagać by oznaczona porcja danych została uruchomiona (np. odczytana w przypadku plików tekstowych lub wykonana w przypadku programów)

w określonym środowisku informatycznym, czy też z zastosowaniem ściśle określonego urządzenia (np. co było już sygnalizowane wyżej, określonego modelu dysku twardego).

6. Próba ustalenia prawa właściwego dla dokonania czynności procesowej podejmowanej w bez-terytorialnej cyberprzestrzeni

Pomimo ustawicznego rozwoju prawa międzynarodowego w zakresie szeroko rozumianych regulacji prawnych cyberprzestrzeni, pośród zagadnień wciąż nierozwiązanych na arenie międzynarodowej (by nie powiedzieć wręcz, że spornych) pozostaje problematyka określania zasad wyznaczania tzw. *cyberjurysdykcji*[45]. O ile wydawać by się mogło, iż ewentualna harmonizacja tzw. prawa komputerowego międzynarodowego, powinna w zasadzie zacząć się od wyznaczenia zasięgu działania poszczególnych państw w cyberprzestrzeni, o tyle proces ten przeprowadzany jest skutecznie głównie w obszarze wspólnego definiowania zagrożeń. Mimo deklaracji, ustawicznie na drugi plan schodzą kwestie związane z ustaleniem szczególnych zasad współdziałania krajów w obszarze zwalczania cyberprzestępczości, zaś jeszcze dalsze miejsce zajmuje kwestia swoistego ustalenia, gdzie zaczyna się, a gdzie kończy, władztwo poszczególnych państw w cyberprzestrzeni.

Bezwątpienia jednym z podstawowych atrybutów każdego państwa - zarówno w ujęciu historycznym, jak i współczesnym, pozostaje faktyczna oraz prawna kontrola nad określonym obszarem ziemi. Kontrola ta wyraża się w szczególności w objęciu obszaru danego państwa jego prawem, które to prawo podlega następnie egzekucji. Ustalając granice terytorium danego kraju, wyznaczane są tym samym granice jego władzy oraz prawa. Zasady te - co było podkreślane w poprzednich rozdziałach pracy poświęconych zagadnieniu *lokalizowania* cyberprzestrzeni, nie dają jednak odnieść się do *logicznego* obszaru cyberprzestrzeni, który wymykając się właściwościom geograficznym, pozostaje *de facto* bez-terytorialnie globalny[46]. Umiejscowione fizycznie elementy infrastruktury sieciowej, jak serwery, węzły łączności, wszelkiego rodzaju urządzenia komutacyjne, czy same sieci telekomunikacyjne, choć tworzą techniczną podbudowę, bez której cyberprzestrzeń nie

---

[45] Terminem tym posługują się coraz częściej przedstawiciele nauki prawnej np. G.Lovet w: *Fighting Cybercrime: Technical, Juridical and Ethical Challenges*, opracowanie dostępne na stronie internetowej pod adresem: http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf, A. Singh w: *Ascertaining Cyber Jurisdiction in Cyber Space: Jurisprudential Understanding and a Comparative Analysis, Social Science Electronic Publishing*, czy E. S. Moore w: *Cyber-jurisdiction, Virginia Lawyer April 2002*.

[46] Więcej na ten temat w: M. Goodman, S. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, s. 7 i nast. Opracowanie dostępne na stronie internetowej pod adresem: http://ijlit.oxfordjournals.org/content/10/2/139.citation).

mogłaby zaistnieć, nie mogą być z cyberprzestrzenią utożsamiane. Wskazywana trudność z pogranicza techniki oraz prawa, w połączeniu z obroną suwerenności oraz ochrony prawnej obywateli, stały się w konsekwencji głównymi przyczynami sygnalizowanego wyżej braku porozumienia międzynarodowego w zakresie ustalenia zasad wyznaczania właściwości prawa krajowego w odniesieniu do czynności dokonywanych w domenie cyfrowej, w tym nie tylko zasad odnoszących się do czynów o charakterze karalnym (cyberprzestępczości), ale także wielu specyficznych czynności z zakresu prawa cywilnego, jak choćby zawierania umów sprzedaży usług sieciowych, uprawiania tzw. *cyberhazardu*, czy świadczenia usług z zakresu ochrony systemów oraz przetwarzanych w nich danych (w tej ostatniej kategorii na pierwszy plan wychodzą zagadnienia gromadzenia oraz przetwarzania danych w tzw. chmurach[47]).

Mając powyższe uwagi za punkt wyjścia dla dalszych rozważań na temat wyznaczania granic jurysdykcji krajowej w cyberprzestrzeni, w pierwszej kolejności należy podkreślić problematyczność stosowania do przedmiotowego problemu rozwiązań prawnych o charakterze ogólnym. Z uwagi na brak regulacji szczególnych, tzw. *cyberjurysdykcja* od strony formalnej musi bowiem opierać się na przepisach odnoszących się do konwencjonalnych metod wyznaczania właściwości prawa krajowego[48]. Co było już podkreślane w niniejszym rozdziale, rozwiązanie takie nastręcza wielu istotnych trudności interpretacyjnych.

Po pierwsze, z uwagi na techniczne zasady funkcjonowania tzw. sieci rozległych - których najistotniejszym przykładem jest Internet, brak jednoznacznych regulacji prawnych stanowiących o metodyce określania cyberjurysdykcji, uzasadnia postawienie podstawowego pytania o samo lokalizowanie czynu wykonywanego w cyberprzestrzeni[49]. Z punktu widzenia użytkownika sieci „miejscem" jego działania jest bowiem fizyczne umiejscowienie komputera, który jest wykorzystywany do przeprowadzenia danej operacji, lub też fizyczna lokalizacja zakończenia sieci, do którego podłączony jest ów komputer (np. zakończenie cyfrowej linii telefonicznej ISDN, koncentryczne gniazdo stałego łącza, wpięty w nie

[47] W pewnym uproszczeniu - dane przetwarzane w chmurach rozsiane są po wszystkich elementach infrastrukturalnych (serwerach, macierzach dyskowych) budujących daną chmurę. Poszczególne serwerownie wykorzystywane przez chmurę mogą być rozsiane po całym świecie, w istocie nierzadko nawet uniemożliwiając jednoznaczne określenie, gdzie określona porcja danych jest rzeczywiście składowana. Istotą chmury jest zatem zupełne oderwanie się od lokalizowania danych w konkretnym systemie, dzięki czemu zasoby chmurowe mogą być wykorzystywane w wysoce elastyczny sposób, z różnych miejsc, przez różne osoby. Więcej na temat chmur (nazywanych też z ang. *cloud computing*) na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Cloud_computing.

[48] E. Galewska, Z. Okoń, M. Ożóg, D. Szostek, M. Świerczyński, E. Trybuchowska, *Cyber Law in Poland,* Wolters Kluwer, Holandia 2011, s. 224 i nast.

[49] M. Kliś, Przestępczość w Internecie. Zagadnienia podstawowe, Czasopismo Prawa Karnego i Nauk Penalnych, Wydawnictwo Polska Akademia Umiejętności, Kraków 2000, opracowanie dostępne na stronie internetowej pod adresem: http://prawo.vagla.pl/node/905.

tzw. *gateway*, czy też modem kablowy, router, router bezprzewodowy itd.). Podstawą opisanego sposobu lokalizowania działań użytkownika cyberprzestrzeni jest oczywiście utożsamianie każdego działania człowieka z chwilową, zawsze aktualną lokalizacją jego osoby. Nawet bowiem działania wykonywane przez człowieka zdalnie (np. wciśnięcie przycisku powodujące wysłanie impulsu elektrycznego, elektromagnetycznego itd.) są przecież inicjowane przez człowieka, którego pozycja poddaje się zawsze możliwości ścisłego określenia współrzędnych geograficznych identyfikujących miejsce jego pobytu (fakt, iż pozycja ta często pozostaje nieznana, nie stanowi o fałszywości powyższego twierdzenia). Innymi słowy - w najbardziej powszechnym rozumieniu, miejscem działania użytkownika cyberprzestrzeni, jest miejsce z którego użytkownik ten uzyskuje dostęp do zasobów cyfrowej domeny.

Po drugie, w przypadku wystąpienia cyberataku, *miejscem zbrodni* definiowanego tym terminem czynu, staje się nie tyle fizyczna lokalizacja osoby, co system teleinformatyczny ofiary lub też system teleinformatyczny przez ofiarę wykorzystywany (np. serwer, na którym znajduje się przełamane konto portalu społecznościowego). O ile bowiem przedmiotem cyberataku mogą stać się bądź dane, bądź też tzw. dostępność systemu (w istocie sprowadzająca się do poprawnego funkcjonowania samego systemu[50]), o tyle każda nieuprawniona operacja, która zostaje dokonana w czasie popełnienia cyberprzestępstwa, musi zostać wprowadzona oraz wykonana przez określony system teleinformatyczny. Tylko systemy mogą bowiem reagować na otrzymywane polecenia, czy zapytania oraz dokonywać operacji na danych. Co warto w tym miejscu przypomnieć, każda operacja sieciowa przeprowadzana jest na zasadzie akcji systemu wywołującego oraz reakcji systemu wywoływanego - dla przykładu, by pobrać dowolne pliki z serwera WWW (jak choćby dla otworzenia strony internetowej), czy też komputera osoby trzeciej, wskazany serwer lub komputer musi zostać *sprowokowany* do ich wysłania, co ostatecznie odbywa się w drodze przeprowadzenia szeregu działań fizycznych, czy wręcz mechanicznych (np. wykonania przez dysk twardy systemu wywoływanego określonej pracy odczytu danych, które następnie są przekazywane dalej). Nie da się bowiem włamać do zasobów komputera, który jest wyłączony z prądu lub nie odpowiada na wysyłane przez sieć zapytania. Można wręcz powiedzieć, że w przypadku przestępstw komputerowych kierowanych przeciwko poufności lub integralności danych, *de facto* systemem „wykonującym" (wprowadzającym w życie)

[50] Należy zaznaczyć, iż w przypadku ataków odmowy dostępu, żadne porcja danych nie musi ulec ani zniszczeniu, ani też nieuprawionemu pozyskaniu, bądź ujawnieniu. Więcej na temat ataków typu DOS oraz DDOW w rozdziale V niniejszej pracy.

czyn przestępny jest sam system atakowany. Z punktu widzenia technicznego, przestępstwa sieciowe wykonywane są w efekcie zawsze pomiędzy dwoma elementami cyberprzestrzeni, z których jeden jest wykorzystywany czynnie przez osobę atakującą, zaś drugi - stanowi zarazem cel i ostateczny przedmiot wykonawczy przestępstwa.

Po trzecie - z uwagi na komercyjną strukturę usług sieciowych oraz charakterystyczne trendy w rozwoju cyberprzestrzeni, wiele spośród zasobów użytkowników systemów teleinformatycznych jest aktualnie przetwarzanych nie tylko lokalnie na ich komputerach (np. dane zapisane na dysku twardym komputera domowego), ale na różnego rodzaju dyskach sieciowych, udostępnianych czy to odpłatnie, czy też darmowo przez podmioty trzecie. Za prosty przykład może tu posłużyć choćby powierzchnia elektronicznej skrzynki pocztowej, która po udostępnieniu przez dostawcę usługi e-mail (np. Onet, Wirtualną Polska, czy Interię - by wymienić przykłady krajowe) może być swobodnie wykorzystywana przez użytkownika do odbierania, przesyłania, a także magazynowania danych komputerowych występujących w dowolnych formatach. Skrzynki pocztowe - podobnie jak wirtualne dyski[51], profile na portalach społecznościowych, czy też blogi lub pokoje czatowe - nie stanowią jednak własności ich użytkownika, lecz własność usługodawcy, który jedynie użycza lub dzierżawi swoje zasoby, uzyskując w zamian korzyści finansowe pochodzące czy to z należności subskrypcyjnych, opłat z tytułu zamieszczanych reklam, czy też w ramach tzw. handlu ruchem sieciowym[52].

Niezależnie od fizycznej lokalizacji użytkownika takich usług, systemy teleinformatyczne wykorzystywane do dostarczania określonych świadczeń mogą znajdować się w dowolnej części świata oraz, co więcej, być obsługiwane przez przedsiębiorcę zarejestrowanego w jeszcze innym kraju (np. niemiecka firma *hostingowa* utrzymująca serwery w Indiach). Prezentowany obraz komplikują dodatkowo kolejne elementy komercyjnej struktury usług sieciowych, w której na świadczenie jednej usługi może składać się wspólna działalność wielu podmiotów, jak np. dostawcy samej usługi sieciowej (podmiotu, który firmuje daną usługę), dostawcy infrastruktury serwerowej, dostawcy oraz *hosta* domeny WWW, czy wreszcie podmiotu administrującego usługą. Sytuacja, w której

[51] Np. usługa Google Drive, pozwalająca na nieodpłatne przechowywanie własnych zasobów na dyskach sieciowych firmy Google. Po założeniu stosownego konta, do którego dostęp podlega ochronie w ramach procesu autoryzacji, użytkownik usługi otrzymuje możliwość wgrywania określonej liczby plików na użyczony lub wydzierżawiony udział sieciowy, do którego może następnie uzyskać dostęp z dowolnego komputera podłączonego do sieci.

[52] Handel ruchem sieciowym polega na odpłatnym przekierowywaniu ruchu pojawiającego się na własnej stronie na inne usługi sieciowe świadczone przez podmioty trzecie. Klasycznym przykładem jest automatyczne otwieranie tzw. wyskakującego okienka z niezamawianą stroną internetową w czasie otwierania innej, oczekiwanej witryny.

występuje mnogość przedsiębiorców nie należy aktualnie do rzadkości.

Przyglądając się zasadom funkcjonowania największych portali usługowych można wręcz zauważyć, iż wysoki stopień specjalizacji w świadczeniu określonych usług sieciowych, powoduje rosnącą dywersyfikację poszczególnych usług pomiędzy różne podmioty, które zmuszone są w efekcie prowadzić symbiotyczną współpracę. Powracając na grunt rozważań prawniczych - należy zauważyć, że definiowane w powyższy sposób usługi stanowią w efekcie szczególny przedmiot cyberprzestępstwa, które będąc kierowane przeciwko dobrom prawnie chronionym użytkownika usługi (np. tajemnica korespondencji), w istocie obiera za cel systemy oraz usługi podmiotów trzecich. Prezentowana struktura powoduje w konsekwencji swoistą wielość podmiotów pokrzywdzonych jednym atakiem, choć ich status w świetle kwalifikacji czynu przestępnego nie zachowuje homogeniczności. Przedstawiany problem obrazują następujące pytania prawne - czyje zabezpieczenia zostają przełamane w momencie przeprowadzania skutecznego ataku na skrzynkę pocztową: użytkownika danej skrzynki, czy podmiotu obsługującego usługę sieciową? Analogicznie, czy włamanie się do konta portalu społecznościowego narusza jedynie prywatność użytkownika przełamanego konta, czy może też prywatność wszystkich osób, które postanowiły udostępnić zaatakowanej osobie określone elementy swoich profilów - jak np. prywatne zdjęcia. Ostatecznie - czy atak odmowy dostępu przeciwko masowej usłudze sieciowej można uznać za kierowany wyłącznie wobec dostawcy usługi, skoro to jej użytkownicy nie mogą z niej korzystać? Powyższe pytania nie znajdują w obecnym stanie prawnym jednoznacznych odpowiedzi, zmuszając - z uwagi na brak regulacji szczególnych, do poszukiwania analogii prawnych pomiędzy obszarem cyberprzestrzeni, a zasadami fizycznego wyznaczania granic terytoriów państwowych. Sygnalizowana struktura usług sieciowych powoduje bowiem faktyczną niemożliwość przypisywania cyberprzestępstw do wyłącznie jednego - choćby logicznego, punktu w cyberprzestrzeni, który mógłby stać się klasycznie pojmowanym „miejscem zbrodni". W pewnym uproszczeniu można bowiem powiedzieć, że cyberprzestępstwo zachodzi wszędzie tam, gdzie naruszone zostaje jakiekolwiek dobro prawnie chronione występujące w obszarze cyberprzestrzeni.

Po czwarte, odwołując się do technicznych zasad organizowania oraz prowadzenia ruchu sieciowego - przedstawionych szerzej w rozdziale III niniejszej pracy, należy zauważyć, iż każdy pakiet danych, który zostaje wysłany przez sieć (w tym pakiet służący za narzędzie do popełnienia cyberprzestępstwa) pokonuje skomplikowaną, sieciową drogę, wykonując szereg skoków po kolejnych węzłach cyberprzestrzeni. Proces ustalania dokładnej ścieżki łączącej dwa dowolnie wybrane punkty cyberprzestrzeni nazywany jest trasowaniem

ruchu (z ang. *trace routing*).

W efekcie przyjęcia powyższej architektury sieci rozległych - do których to sieci w szczególności należy Internet, pakiet danych służących za narzędzie sprawcze do przeprowadzenia cyberataku, przechodzi przez liczne elementy sieciowe, ostatecznie docierając do systemu atakowanego z pozycji ostatniego z węzłów pośredniczących, układających się w ścieżkę obsługi danego połączenia cyberprzestrzeni. Innymi słowy, ustalając bezpośrednie źródło pakietów danych, które stały się narzędziem ataku, dociera się nie tyle od systemu sprawcy, co jednego z serwerów pośredniczących w wymianie danych, obsługiwanych najczęściej przez przedsiębiorców telekomunikacyjnych, w tym dostawców sieci. Przekierowywanie ruchu sieciowego może wreszcie także stanowić umyślny zabieg sprawcy ataku, który chcąc dodatkowo ukryć swoje dane, może posłużyć się jedną z wielu technologii anonimizacji ruchu, jak choćby serwerami proxy, czy też usługą tzw. trasowania cebulowego[53]. O ile dalsze, zwrotne śledzenie trasy, którą pokonały przedmiotowe pakiety danych jest oczywiście możliwe (na zasadzie podążania „po nitce do kłębka”), o tyle zarysowywany problem powoduje istotne wątpliwości w zakresie ustalania prawa właściwego do przeprowadzenia samej kwalifikacji karnej danego czynu. W pierwszej kolejności, nasuwa się pytanie, czy określony rodzaj ataku musi stanowić czyn zabroniony ustawą w każdym z krajów, który mimowolnie stał się gospodarzem systemów pośredniczących, przesyłających dalej ruch sieciowy w sposób w pełni zautomatyzowany? Pytanie to nabiera szczególnego znaczenia w odniesieniu do ataków opierających się na specyficznych formach wykorzystania powszechnie dostępnych, legalnych funkcji sieciowych - które w rękach hackerów mogą stanowić narzędzi zbrodni. Po drugie, czy można uznać właściwość organów ścigania dowolnego z państw-gospodarzy systemów pośredniczących, czy może jedynie państwa pierwszego lub też ostatniego w ścieżce wymiany danych? I wreszcie po trzecie - czy uznanie właściwości któregokolwiek z porządków prawnych pozwala na jakąkolwiek ingerencję prawną w jurysdykcję pozostałych państw - innymi słowy, czy określenie danego państwa jako właściwego do przeprowadzenia określonego postępowania, może być rozumiane, jako wyłączające konieczność potwierdzania podwójnej karalności, czy też uprawniającego do prowadzenia działań w zasobach cyberprzestrzeni, które przetwarzane są na serwerach zlokalizowanych poza granicami tego kraju? Obok oczywistego wymogu stosowania w tej sytuacji instytucji pomocy prawnej, zarysowuje się tu bowiem mniej wyraźny problem, ustalenia, czy dane państwo w ogóle posiada tytuł prawny do występowania o wsparcie

---

[53] Więcej o metodzie na stronie internetowej pod adresem: http://pl.wikipedia.org/wiki/Trasowanie_cebulowe.

swoich działań procesowych. Analogiczne stosowanie ogólnych zasad prawa karnego procesowego do opisanych wyżej sytuacji, nie pozwala niestety na udzielenie jednoznacznych odpowiedzi na tak sformułowane pytania. Konieczność stosowania regulacji, które powstały z myślą o uznawania *stricte* fizycznych granic państwowych prowadzi jedynie do ogólnych wniosków o konieczności wydatnego stosowania instytucji pomocy prawnej przy znakomitej większości przestępstw popełnianych w cyberprzestrzeni, które z uwagi na specyfikę domeny cyfrowej - niezwykle często stają się przestępstwami międzynarodowymi. Ostatecznie zatem o przyjęciu właściwości określonego porządku prawnego dla prowadzenia postępowania, będą decydowały zasady współpracy poszczególnych krajów, określane przede wszystkim umowami dwu lub wielostronnymi. Swoistą próbą rozwiązania powyższego problemu stały się odnośne postanowienia Konwencji Budapesztańskiej o cyberprzestępczości[54], które w zakresie procesowym (w tym jurysdykcyjnym) nie znalazły jednak szerokiej implementacji, która stałaby się zalążkiem do wytworzenia wspólnego, ponadnarodowego systemu szczególnej współpracy karnej w sprawach o czyny popełnione w cyberprzestrzeni.

Ostatecznie, piątym obszarem, wywołującym istotne trudności w analogicznym stosowaniu przepisów ogólnych - konstytuujących podstawowe zasady określania prawa właściwego, w stosunku do czynów popełnionych w obszarze cyberprzestrzeni, jest problematyka związana ze sposobem ujawniania faktu popełnienia cyberprzestępstwa. W praktyce bowiem, ataki skierowane przeciwko poufności lub integralności danych najczęściej ujawniane są w drodze zalogowania się uprawnionego użytkownika systemu, czy to do własnego komputera, czy też stosownej usługi sieciowej, której zasoby zostały skompromitowane. Niezależnie zatem od szczegółowej konfiguracji okoliczności opisujących określone zdarzenie przestępne (np. tego, czy uszkodzony plik znajdował się lokalnie na maszynie ofiary, czy też na dysku sieciowym, do którego ofiara posiada dostęp), pierwszy ujawniony egzemplarz danych potwierdzających fakt popełnienia czynu zabronionego w cyberprzestrzeni, zapisuje się na komputerze ofiary chcącej uzyskać uprawiony dostęp do wybranych, zaatakowanych zasobów. Innymi słowy, fakt popełnienia cyberprzestępstwa - bez względu na miejsce lokalizujące w sposób fizyczny nośnik, na którym przetwarzane są zaatakowane dane, najczęściej manifestuje się po raz pierwszy w systemie teleinformatycznym ofiary ataku, która stwierdza wystąpienie szeroko rozumianych nieprawidłowości w sposobie przetwarzania określonej porcji danych. To w tym bowiem momencie dochodzi do rzeczywistego ustalenia naruszenia praw, w tym dóbr osobistych

[54] Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

określonego użytkownika - człowieka.

Mając powyższe na uwadze, można dojść do wniosku, iż niezależnie od fizycznych lokalizacji systemów: atakowanego oraz atakującego, cyberprzestępstwo odnoszące się przecież do ochrony dóbr prawnych określonych osób fizycznych lub osób prawnych, *de facto* w pewnym sensie urzeczywistnia się w lokalizacji ofiary, która wbrew swoim uprawnieniom nie może skorzystać z danego zasobu cyberprzestrzeni w sposób zgodny z jego przeznaczeniem, czy też zastosowaniem. Co ważne, uprawnienie to pozostaje równie aktualne w miejscu zamieszkania ofiary, jak również każdym innym, w którym ofiara ta aktualnie się znajduje, próbując uzyskać dostęp do uszkodzonych, wykradzionych lub też w inny sposób naruszonych zasobów cyberprzestrzeni. Zaprezentowane spojrzenie podważa w całości możliwość odnoszenia wymiarów geograficznych w stosunku do kwestii ustalania prawa właściwego dla identyfikacji sytuacji prawnej określonego zdarzenia przestępnego, popełnionego w obszarze cyberprzestrzeni.

Podsumowując powyższe rozważania należy zauważyć, iż problematyka prawna odnosząca się do zagadnień wyznaczania tzw. cyberjurysdykcji, skłania do wyrażenia poglądu, iż standardowe regulacje prawne - przyjmujące za punkt wyjściowy dla ustalenia zasięgu jurysdykcji poszczególnych państw kształt ich granic zewnętrznych, nie pozwalają na rozwiązywanie podstawowych problemów określania prawa właściwego w obszarze cyberprzestrzeni. Stosując owe regulacje ogólne, można bowiem dojść do w zasadzie dowolnych wniosków, uprawniających choćby tezę o właściwości każdego z państw, którego systemy brały jakikolwiek udział w procesie realizacji zdarzenia przestępnego. Docelowe zasady określania cyberjurysdykcji powinny natomiast pozwalać na ścisłe ustalenie, podług którego systemu prawnego dany czyn winien być identyfikowany, zapewniając tym samym gwarancję pewności prawa, w zakresie oceny co jest dopuszczalne w danym „obszarze" sieci, a co nie. Tak bowiem jak globalna jest sama cyberprzestrzeń, tak też pan-światowe powinny być zasady prawne rządzące cyberprzestrzenią.

§2. Podejmowanie czynności przeszukania oraz zatrzymania rzeczy w cyberprzestrzeni

Zgodnie z przyjętą budową niniejszego rozdziału pracy, jego druga część została poświęcona zagadnieniom szczególnej problematyki podejmowania w cyberprzestrzeni podstawowych czynności procesowych o charakterze dowodowym - to jest czynności przeszukania oraz zatrzymania rzeczy. Mając powyższe uwagi o charakterze ogólnym za punkt wyjścia do dalszych rozważań, możliwe staje się przedstawienie dynamicznego ujęcia wybranych czynności procesowych na gruncie tak prawnym, jak również faktycznym - który

z uwagi na wysoki stopień specjalizacji dziedziny informatyki, istotnie uzupełniany jest podstawami technicznymi. Dla uniknięcia powtórzeń, wcześniejsze rozważania o charakterze ogólnym będą w dalszej części rozdziału jedynie przywoływane. Z uwagi na specjalistyczny charakter pracy - niniejsze opracowanie skupia się wyłącznie na kwestiach szczególnych dla problematyki podejmowania wybranych czynności procesowych w obszarze cyberprzestrzeni, pomijając zaś uwagi ogólne na ich temat, w zakresie w jakim nie wpływa to na przejrzystość prowadzonego wywodu.

1. Problematyka karno-procesowa prowadzenia czynności przeszukania w cyberprzestrzeni

Z uwagi na coraz powszechniejsze wykorzystywanie najróżniejszego rodzaju elektronicznych urządzeń teleinformatycznych - manifestujących swoje miejsce nawet w trakcie wykonywania czynności życia codziennego, problematyka przeszukiwania zasobów cyberprzestrzeni stała się aktualnie istotnym problemem faktycznym, z którym muszą mierzyć się organy ścigania. Nowoczesne możliwości przetwarzania ogromnych ilości danych - zapisywanych nie tylko lokalnie na komputerach będących w fizycznym władaniu ich właścicieli, ale także w szeroko rozumianych zasobach cyberprzestrzeni, których elementy infrastrukturalne mogą być rozrzucone po całym świecie - powodują jednocześnie szereg problemów prawnych związanych z wyznaczeniem zakresu oraz zasięgu czynności procesowych realizowanych w cyberprzestrzeni. Przeszukiwanie zasobów cyfrowych to bowiem nie tylko fizyczne zabezpieczanie nośników danych (dokonywane analogicznie jak zabezpieczenie dowolnego przedmiotu), ale także przeszukiwanie samych danych pod kątem ujawniania oraz zabezpieczania dowodów występujących w postaci elektronicznej - zarówno tych zapisanych lokalnie, jak i tych przetwarzanych w cyberprzestrzeni, do których dostęp uzyskuje się pośrednio z wykorzystaniem w istocie dowolnego systemu teleinformatycznego. Przeszukanie takie obejmuje swoją specyfiką *de facto* szereg czynności, a zatem nie tylko proste oględziny danych - ich czytanie, ale także wyszukiwanie w zabezpieczonym materiale określonych danych (plików) po słowach kluczowych, ujawnianie danych ukrytych, czy wreszcie ujawnianie treści materiałów zabezpieczonych z wykorzystaniem technik kryptograficznych[55]. Co wymaga także podkreślenia, jako uwaga wstępna, pojęcie przeszukiwania zasobów cybernetycznych nie może być ograniczane przedmiotowo do

[55] Na problemy te uwagę zwraca A. Lach w: Prawa i obowiązki dysponentów i użytkowników systemu informatycznego w związku z jego przeszukaniem i zatrzymaniem danych. Pełny tekst opracowania dostępny na stronie internetowej pod adresem: http://www.secure.edu.pl/historia/2005/docs/26.10/07_lach /lach-r.pdf.

przeszukiwania standardowych komputerów, bowiem obejmuje swoim zakresem wszelkie urządzenia służące do przetwarzania danych w postaci cyfrowej - a zatem także urządzeń sieciowych, serwerów, cyfrowych central telefonicznych, tabletów, smartfonów oraz szeregu innych urządzeń wyposażanych w karty pamięci bądź też inne informatyczne nośniki danych[56].

Dostrzegając sygnalizowane wyżej wyzwania, ustawodawca polski jeszcze w 2003 r. wprowadził do Kodeksu postępowania karnego[57] przepis art. 236a, który po dodatkowej zmianie w roku 2004[58], uzyskał ostatecznie brzmienie, stanowiące iż:

> „236a. Przepisy rozdziału niniejszego [rozdziału 25 - zatytułowanego „Zatrzymanie rzeczy. Przeszukanie" - przyp. autora] stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną.".

Obok wyraźnego objęcia problematyki przeszukiwania zasobów elektronicznych zakresem analogicznego stosowania przepisów ogólnych dotyczących przeszukania oraz zatrzymania rzeczy, pierwszą z wymienionych nowel wprowadzone zostały także drobne modyfikacje w budowie owych przepisów ogólnych, mające na celu unowocześnienie struktury prawnej konwencjonalnych czynności procesowych do nowych wyzwań, jakie stawia między innymi zjawisko cyberprzestępczości. W szczególności, zmodyfikowane zostały w tym zakresie regulacje traktujące o pozyskiwaniu treści pochodzących z „korespondencji przesyłanej pocztą elektroniczną" w ramach czynności procesowej kontroli i utrwalania rozmów (*vide* znowelizowany wówczas przepis art. 241 Kodeksu postępowania karnego). Jak zostało wskazane w uzasadnieniu do ustawy zmieniającej: „Świadectwem czasu jest propozycja, aby przepisy o zatrzymaniu rzeczy i przeszukaniu stosować odpowiednio do dysponenta i użytkownika systemu informatycznego w zakresie danych przechowywanych w tym

---

[56] Materiały Komendy Głównej Policji - Wydziału Wsparcia Zwalczania Cyberprzestępczości Biura Kryminalnego, na temat czynności przeszukania systemu teleinformatycznego, dostępne na stronie internetowej pod adresem: http://www.policja.pl/pol/kgp/biuro-sluzby-kryminaln/cyberprzestepczosc/74488,Przeszukanie-i-zatrzymanie-rzeczy-udzial-specjalistow-i-bieglych-w-czynnosciach-.html.

[57] Wskazywana zmiana została wprowadzoną ustawą z dnia 10 stycznia 2003 r. o zmianie ustawy – Kodeks postępowania karnego, ustawy – Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych (Dz. U. Nr 17, poz. 155 z późn. zm.). Tekst noweli dostępny na stronie internetowej pod adresem: http://isap.sejm.gov.pl/DetailsServlet?id=WDU20030170155.

[58] Ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz. U. Nr 69, poz. 626). Pełny tekst ustawy dostępny na stronie internetowej pod adresem: http://isap.sejm.gov.pl/DetailsServlet?id=WDU20040690626.

systemie lub na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji już przesłanej pocztą elektroniczną (art. 236a)”[59].

Druga z wymienionych ustaw - to jest nowela z 2004 r., stała się natomiast głównym narzędziem prawnym implementującym do porządku krajowego postanowienia wielokrotnie już przywoływanej, budapesztańskiej Konwencji o Cyberprzestępczości[60], wprowadzając nie tylko szereg nowych typizacji przestępstw do Kodeksu karnego, ale także zestaw nowych przepisów Kodeksu postępowania karnego, mających na celu w szczególności zabezpieczenie poprawnego przebiegu postępowania w sprawach o przestępstwa popełnione w obszarze cyberprzestrzeni (z uwagi na zakres niniejszego rozdziału, zagadnienia te prezentowane są nieco dalej). Oceniając przyjęty przez ustawodawcę zabieg legislacyjny, polegający na wprowadzeniu nakazu odpowiedniego stosowania przepisów ogólnych w stosunku do czynności podejmowanych w stosunku do szeroko rozumianych zasobów teleinformatycznych - należy zauważyć, iż pomimo jego niewątpliwej wartości w zakresie wyznaczenia ram prawnym dla przedmiotowego problemu (była to pierwsza regulacja w analizowanym zakresie), zaproponowany przepis nie stanowił - i co potwierdziły tylko kolejne lata nie stanowi, rozwiązania pozbawionego wad. Podejmowana w niniejszej pracy specyfika cyberprzestrzeni - prezentowana w istocie na przestrzeni wszystkich rozdziału opracowania, nie dała bowiem zamknąć się w prostym wyrażeniu prawnym konstytuującym jej „odpowiedniość” do *świata fizycznego*, który pozostaje poznawalny z wykorzystaniem samych tylko ludzkich zmysłów, nie wymagając zaś korzystania z urządzeń informatycznych[61]. Niemniej, przyjęte w roku 2003 oraz uzupełnione w roku kolejnym rozwiązanie ustawodawcze, do dziś pozostało głównym punktem wyjścia do rozważań na temat podejmowania w cyberprzestrzeni czynności przeszukania oraz zatrzymania. Na tle owych rozważań zarysowuje się jednak w piśmiennictwie szereg rozbieżności, co do sposobu rozumienia oraz realizowania „odpowiedniego” stosowania przepisów rozdziału 25. Kodeksu postępowania karnego wobec czynności wykonywanych w domenie cyfrowej, z których najpoważniejsze dotykają kwestii możliwości bezstratnego powielania danych stanowiących dowody oraz związaną z tym pośrednio możliwość wykonywania przeszukań *on-line*.

---

59 Prace Sejmu RP IV kadencji – druk sejmowy Nr 182, s. 60. Powtarzam za: M. Zelek, Przeszukanie urządzenia zawierającego dane informatyczne lub systemu informatycznego w świetle polskiego procesu karnego. Tekst opracowania dostępny na stronie internetowej pod adresem: http://www.edukacjaprawnicza.pl/aktualnosci/a/pokaz/c/aktualnosc/art/przeszukanie-urzadzenia-zawierajacego-dane-informatyczne-lub-systemu-informatycznego-w-swietle-polskiego-procesu-karnego.html.

60 Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

61 Wskazywane problemy identyfikuje jednoznacznie A. Lach w: Prawa i obowiązki dysponentów..., op. cit.

Przechodząc na grunt analizy prawnej samego przepisu art. 236a Kodeksu postępowania karnego, należy zauważyć, iż zgodnie z jego obecnym brzmieniem, przepis ten odnosi się w pierwszej kolejności do „dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego". Pomimo niejednoznacznej redakcji przepisu - pozwalającej na rozdzielenie pojęć *dysponent i użytkownik urządzenia* od pojęcia *system informatyczny,* co nadaje drugiemu z nich charakteru samodzielnego podmiotu, problem ten nie został poddany należytym badaniom ze strony przedstawicieli doktryny prawniczej. Faktyczne stosowanie dyspozycji przepisu art. 236a zostało tym samym odniesione w większości opracowań do samych osób dysponenta i użytkownika, pomijając istotną możliwość interpretacji przepisu w zakresie podejmowania czynności przeszukania odpowiednio wobec nie tylko osób, ale także samego systemu informatycznego. Uwaga ta znajduje swoje rozwinięcie w dalszej części rozdziału, poświęconej zagadnieniu wykonywania czynności zdalnego przeszukania systemu, to jest przeszukania wykonywanego za pośrednictwem cyberprzestrzeni, a bez fizycznego styku z badanym nośnikiem danych.

Analizując niezdefiniowane prawnie pojęcia „dysponent" oraz „użytkownik", należy podzielić pogląd, iż pierwsze z nich odnosi się do osoby upoważnionej do dysponowania systemem (np. jego właściciel, czy też wskazany przez właściciela administrator), zaś drugie - do każdej z osób, która faktycznie wykorzystuje dany system[62] zgodnie z posiadanymi uprawnieniami oraz zasadami pracy obowiązującymi w tym systemie lub danej usłudze sieciowej (np. użytkownik konta poczty elektronicznej, gość strony WWW, posiadacz profilu na portalu społecznościowym, czy wreszcie użytkownik komunikatora internetowego)[63]. Odniesienie przepisu do wskazanych wyżej osób implikuje *de iure* konieczność podejmowania czynności przeszukania lub zatrzymania danych nie tyle w stosunku do samych danych, co właśnie wskazanych osób, posiadających określony dostęp do wybranych zasobów. Następstwem przedstawionej interpretacji jest ograniczanie możliwości prawnych pozyskiwania danych przetwarzanych w systemach zamkniętych (w przeciwieństwie do zasobów publicznych, dostępnych dla wszystkich użytkowników cyberprzestrzeni, jak choćby otwarte strony WWW), które dokonywane byłoby bez żadnego udziału osób trzecich, w szczególności zaś dysponenta lub użytkownika systemu. Jak zauważa A. Lach - „Zakres przedmiotowy odpowiedniego stosowania przepisów rozdziału 25 KPK ograniczony został do danych przechowywanych w systemie lub na nośniku i znajdujących się w dyspozycji lub

62 Na konstytuujący status „użytkownika systemu" aspekt faktycznego wykorzystywania tego systemu, uwagę zwraca M. Zelek, op. cit.

63 Tak np. K. T. Boratyńska w: K. T. Boratyńska, A. Górski, A. Sakowicz, A. Ważny, Kodeks postępowania karnego. Komentarz, C. H. Beck, Warszawa 2012, wyd. 4, s. 523.

użytkowaniu wskazanych wyżej osób. Oznacza to, że w razie żądania wydania danych, powinny one być w zasięgu określonej osoby [...] byleby tylko osoba ta w sposób legalny mogła spowodować ich przesłanie, skopiowanie, edycję itp. Dane te nie muszą także znajdować się na terytorium Polski, mogą to być np. dane przechowywane w skrzynce pocztowej znajdującej się na serwerze zagranicznym. Dostęp do danych znajdujących się za granicą może uzyskać jednak jedynie uprawniona osoba, a nie organ procesowy, który musiałby działać w ramach procedur pomocy prawnej, chyba że dane mają charakter ogólnodostępny"[64]. W świetle przytoczonego poglądu - wiązanie w przepisie art. 236a Kodeksu postępowania karnego czynności przeszukania systemu z osobą jego dysponenta lub użytkownika, oznacza tym samym zakaz samodzielnego sięgania przez organy procesowe po zasoby teleinformatyczne lokalizowane poza granicami kraju - co z uwagi na specyfikę cyberprzestrzeni stanowi sytuację nagminną. Swoiste, choć nie w pełni kompletne, rozwiązanie opisywanej sytuacji zapewniają regulacje szczególne odnoszące się w pierwszym rzędzie do przedsiębiorców telekomunikacyjnych oraz podmiotów świadczących usługi telekomunikacyjne, na których nałożone zostały obowiązki zatrzymywania oraz wydawania określonych kategorii danych (np. przepis art. 218 oraz 218a Kodeksu postępowania karnego). Co istotne, możliwość odcięcia dyspozycji art. 236a Kodeksu postępowania karnego od osób fizycznych dysponenta lub użytkownika systemu - a zatem dopuszczenie stosowania tego przepisu wobec przeszukania samego systemu (co wydaje się dopuszczalne w świetle redakcji art. 236a), mogłaby stanowić skuteczną odpowiedź na zjawisko ukrywania danych stanowiących przedmiot przestępstwa komputerowego na zlokalizowanych poza granicami kraju systemach, do których uzyskanie dostępu wymaga uzyskania tzw. autoryzacji, w szczególności wyrażającej się we wprowadzeniu poprawnego hasła. Kwestia ta jednak - jak zresztą zauważa ponownie A. Lach - wymagałby ścisłych regulacji prawnych, wykluczających możliwości nadużyć ze strony organów procesowych podejmujących czynności w obszarze cyberprzestrzeni[65]. Odnoszenie zasad regulujących prowadzenie przeszukania wprost do systemu informatycznego, wymagałoby wreszcie także określenia w postaci przepisów szczególnych, dopuszczalnych form prawnych interakcji z tego typu elementami cyberprzestrzeni, stanowiącymi nietypowy - bo nienamacalny rodzaj rzeczy. Zagadnienie prowadzenia tzw. przeszukania na odległość opisane zostało szerzej w dalszej części rozdziału.

---

[64] A. Lach, Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego, Prok. i Pr. 2003, Nr 10, s. 16–25, przytaczam za: M. Zelek, op. cit.

[65] A. Lach, Przeszukanie na odległość systemu informatycznego, Prokuratura i Prawo 2011, s. 67 i nast. Tekst opracowania dostępny na stronie internetowej pod adresem: http://prawo.uni.wroc.pl/pliki/13373.

Przedmiotem czynności określonych w art. 236a Kodeksu postępowania karnego są „dane przechowywane w [...] urządzeniu lub systemie albo na nośniku znajdującym się w jego [użytkownika lub dysponenta systemu] dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną". Zgodnie z przyjętą redakcją przepisu, przedmiotem poszukiwanym w czasie czynności przeszukania szeroko rozumianych zasobów cyberprzestrzeni, są zatem dane, które mogą być zapisane zarówno w systemach, jak i dowolnych nośnikach. O ile *de facto* każde dane przetwarzane są z zastosowaniem określonego rodzaju nośnika (nawet dane nie zapisywane trwale na dysku muszą zaistnieć w pamięci operacyjnej komputera - RAM, czy choćby pamięci podręcznej procesora - CACHE), o tyle zastosowaną w przepisie formułę należy rozumieć, jako wykluczającą wątpliwości co do różnego traktowania nośników tzw. wewnętrznych (np. wbudowane dyski) od tych zewnętrznych, które po odłączeniu od komputerów lub innych urządzeń tracą charakter elementu systemu teleinformatycznego, stając się samodzielnym urządzeniem. Analogicznie należy też rozumieć wpleciony w przepis zwrot „w tym korespondencji przesyłanej pocztą elektroniczną", która to korespondencja stanowi oczywiście takie same dane komputerowe, jak każdy inny przetwarzany cyfrowo materiał. Korespondencja jest bowiem wyłącznie jedynym z rodzajów treściowych, który mogą przybrać takie dane. Samo wyrażenie „korespondencja przesyłana" nie może być wreszcie także rozumiany, jako odnoszący się do korespondencji już wysłanej, czy tez podlegającej wysłaniu w danej chwili, lecz raczej do korespondencji, która w ogóle podlega wysyłaniu poprzez sieci, a zatem każdej postaci w której tylko występuje wiadomość e-mail[66].

Komentowany przepis art. 236a Kodeksu postępowania karnego posługuje się wreszcie także niezdefiniowanymi prawnie kategoriami „urządzenia zawierającego dane informatyczne" oraz „systemu informatycznego" - które to pojęcia mają wyznaczać zakres oddziaływania obowiązującej regulacji. Mając na uwadze wcześniejsze rozważania definicyjne, zawarte w poprzednich rozdziałach pracy, wprowadzoną do przepisu siatkę terminologiczną należy uznać za chybioną, bowiem posługującą się pojęciami nieostrymi, pozbawionymi swoich normatywnych definicji. Co stanowiło przedmiot wcześniejszych szczegółowych rozważań, podstawowym pojęciem stosowanym na gruncie prawa krajowego na określenie szeroko rozumianych elementów cyberprzestrzeni jest zwrot „system teleinformatyczny". Samo zaś pojęcie „systemu informatycznego" - wbrew legislacyjnemu

---

[66] Tak właśnie: A. Lach w: Prawa i obowiązki dysponentów..., op. cit., s. 2.

celowi wprowadzenia przepisu art. 236a, którym miała przecież być implementacja postanowień Konwencji o Cyberprzestępczości do polskiej ustawy - nie znajdowało w oryginalnym brzmieniu konwencji swojego odpowiednika. Przywołany akt międzynarodowy posługuje się bowiem w oryginale terminem „systemy komputerowe"[67], który to termin dopiero w oficjalnym tłumaczeniu Konwencji, sporządzonym na potrzeby jej ratyfikacji do polskiego porządku prawnego (co ostatecznie nastąpiło dopiero w 2016 r.), został przetłumaczony na wyrażenie „system informatyczny" niejako sankcjonując błędnie wykonane tłumaczenie przyjęte na potrzeby znacznie wcześniejszej ustawy nowelizującej Kodeks postępowania karnego.

Przechodząc do zagadnień prawnych związanych z samą realizacją czynności przeszukania systemów teleinformatycznych, należy zauważyć, iż czynność ta, wykonywana na podstawie postanowienia sądu lub prokuratora, powinna rozpoczynać się od wezwania dysponenta lub użytkownika systemu do wydania określonych danych - co stanowi efekt odpowiedniego stosowania w tym zakresie przepisu art. 217 Kodeksu postępowania karnego. Należy wyrazić pogląd, iż w przypadku dobrowolnego wydania danych przez osobę wezwaną do wykonania czynności, traci znaczenie fakt, gdzie określone dane były przechowywane w chwili realizacji czynności. O ile zatem osoba wezwana np. samodzielnie loguje się na skrzynkę pocztową funkcjonującą w usłudze poczty amerykańskiej *Gmail*, oraz dobrowolnie wykonuje kopię listów i wręcza ją przedstawicielom organów ścigania - o tyle nie zachodzi w tej sytuacji naruszenie zasad udzielania międzynarodowej pomocy prawnej, bowiem pobrany materiał został uzyskany i zabezpieczony w kraju, bez naruszenia jakichkolwiek zasad technicznych funkcjonowania danej usługi sieciowej i co więcej - po uzyskaniu do niego dostępu oraz zapisaniu przez uprawnionego dysponenta systemu (usługi), będącego w tym wypadku klientem usługi sieciowej. Co istotne, z uwagi na wskazaną wcześniej możliwość bezstratnego powielania danych (wykonywania nieskończonych liczb kopii, w tym kopii z kopii), nie wydaje się zasadne aby przyjmować pogląd o konieczności wydania danych na oryginalnym nośniku, na którym po raz pierwszy pojawiły się w otoczeniu osoby pozyskującej dane. Nie powinno być zatem odbierane jako naruszające zasady sztuki kryminalistycznej odebranie rzeczonej wiadomości poczty elektronicznej w postaci jej kopii, zapisanej np. na zewnętrznym nośniku (pamięci typu *pendrive*), dostarczonym choćby przez sam organ procesowy. Prezentowany pogląd dotyczący zabezpieczania wyłącznie kopii

[67] W oryginale, z ang. „*computer system*". Pojęcie to zostało zdefiniowane w art. 1 lit. a konwencji. Pełny tekst dokumentu dostępny jest na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

danych nie znajduje jednak pełnego poparcia pośród przedstawicieli doktryny, którzy podnoszą iż stosując w tym zakresie analogię, zamiast dokumentów papierowych można byłoby pozyskiwać w ramach przeszukania wyłącznie ich kserokopie[68].

Przytoczony argument wydaje się jednak nietrafiony, bowiem o ile kserokopia materiału papierowego, jak również wydruk dokumentu z komputera[69], traci nie tylko technicznie, ale także formalnie charakter oryginału (skserowany podpis nie posiada mocy oryginalnego podpisu odręcznego), o tyle skopiowane dane stanowią idealne powielenie materiału kopiowanego, posiadając cechy identyczne jak materiał pierwotny (w przypadku kopii dokumentu opatrzonego podpisem elektronicznym ów podpis również podlega kopii). Po wykonaniu kopii oraz usunięciu pliku, z którego kopia została wykonana, dane kopiowane mogą zatem z powodzeniem funkcjonować, jak jedyny oryginalny egzemplarz pliku bądź innego materiału, pod warunkiem tylko, że zostały skopiowane w sposób zapewniający identyczność nie tylko samych danych, ale również opisujących je tzw. metadanych[70], wskazujących np. datę utworzenia pliku (technicznie, stosuje się w tym celu specjalne rozwiązania sprzętowe[71], nazywane blokerami). Powyższe rozumowanie dopuszczalne jest od strony prawnej z uwagi na nakaz „odpowiedniego" stosowania przepisów o przeszukaniu do przeszukania odnoszącego się do zasobów informatycznych, co oznacza wręcz konieczność stosowania przepisów nie wprost, ale z wymaganymi zmianami, uwzględniającymi specyfikę odnośnych czynności - w tym zatem wypadku, specyfikę pozyskiwania szeroko rozumianych danych komputerowych.

Powyższa sytuacja ulega jednak istotnym komplikacjom prawnym oraz faktycznym w przypadku braku dobrowolności poddania się czynnościom przeszukania ze strony osoby wezwanej do jej realizacji. Należy bowiem pamiętać, iż osoba wzywana do wydania rzeczy nie ma obowiązku prawnego współpracy z organem procesowym, zaś jedynie obowiązek prawny poddania się czynnościom, a zatem znoszenia faktu jej prowadzenia (obowiązek określany terminem *pati*). Zasada ta stanowi w istocie faktyczne wdrożenie konstytucyjnej zasad *nemo se ipsum*[72].

Pośród głównych trudności o charakterze technicznym należy wskazać w szczególności na:

---

[68] Tak np. M. Zelek, op. cit.

[69] W piśmiennictwie zaznacza się, iż wydruk przybiera postać dokumentu w przypadku, gdy jest podpisany, tak np. B. Fischer, Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalisytczne, Zakamycze, Kraków 2000, s. 117.

[70] M. Cross, D. Littlejohn Shinder, op. cit., s. 122 i nast.

[71] Szerzej na temat budowy tzw. kryminalistycznego stanowiska badawczego B. Fischer, op. cit., s. 122 i nast.

[72] Kwestię tę słusznie zaznacza M. Zelek, op. cit.

- możliwość zabezpieczania przeszukiwanych danych z zastosowaniem technik kryptograficznych, co powoduje obiektywną niemożliwość realizacji czynności, występującą do czasu odszyfrowania danych. Proces ten wymaga zastosowania wiedzy specjalistycznej oraz może być wysoce czasochłonny w przypadku wystąpienia konieczności odszyfrowania dużych woluminów danych,
- możliwą konieczność uzyskiwania dostępu do danych przetwarzanych w usługach sieciowych, zabezpieczonych w szczególności hasłami autoryzującymi użytkownika. Wiele spośród stosowanych zabezpieczeń powoduje blokadę usługi w przypadku ustalenia w systemie próby uzyskania dostępu ze strony osoby innej, niż pierwotnego użytkownika. Np. trzykrotne wpisanie niepoprawnego hasła może powodować zablokowanie konta na 24 h, uniemożliwiając tym samym realizację czynności przeszukania w miejscu jej podjęcia,
- potencjalną - choć w praktyce wysoce prawdopodobną, konieczność uzyskiwania dostępu do zasobów lokalizowanych poza granicami kraju,
- możliwą konieczność przeszukiwania ogromnych woluminów danych, w tym też rozsianych po wielu nośnikach, jak np. danych przetwarzanych w macierzach dyskowych, na które mogą składać się nawet setki połączonych nośników, co powoduje, iż zachowane na nich dane zapisane są w sposób fragmentaryczny (jeden plik może być zapisany w wielu częściach rozłożonych na wielu dyskach twardych),
- znajomość zasad technicznych odczytywania danych o wielu różnych, często wysoce specjalistycznych formatach, które to dane mogą występować nie tylko w postaci zapisu na trwałych nośnikach pamięci (np. na dysku twardym), ale także być przetwarzane wyłącznie w pamięci ulotnej (np. pamięci operacyjnej komputera - RAM), wymagającej szczególnego traktowania celem uniknięcia nieumyślnej modyfikacji lub wręcz całkowitego zniszczenia dowodu, oraz wreszcie,
- możliwość wystąpienia konieczności poszukiwania na nośnikach śladów danych usuniętych, jednak nie wyczyszczonych z pamięci w sposób permanentny.

Zarysowujące się na powyższym tle technologicznym problemy prawne to odpowiednio:

- konieczność odszyfrowania danych, co może nastąpić bądź to w drodze powołania biegłych do przeprowadzenia czynności dekryptażu, związaną z koniecznością uprzedniego zatrzymania partii zaszyfrowanych nośników (w przypadku braku ustalenia relewantności uzyskanych tą drogą materiałów, organy procesowe mogą narażać się na zarzut nadmiernej ingerencji w prawa obywatela, któremu np. zabierane

są całe macierze dyskowe) bądź też poprzez spowodowanie wydania niezbędnych haseł lub też innych danych, wymaganych do uzyskania dostępu badanych zasobów[73],

- konieczność uzyskiwania wydatnego wsparcia ze strony podmiotów obsługujących usługi sieciowe, w szczególności przedsiębiorców telekomunikacyjnych,
- konieczność działania w ramach instytucji pomocy prawnej, opierającej w wymiarze pragmatycznym na jakości współpracy pomiędzy określonymi państwami oraz czasach ich reakcji,
- prowadzenie tzw. przeszukania rozszerzonego, którego zakres zwiększa się na kolejne systemy nieobjęte pierwotnym planem przeszukania, a w szczególności postanowieniem sądu lub prokuratora, oraz ostatecznie
- konieczność realizacji czynności przez odpowiednio przygotowanych oraz wyposażonych specjalistów, którzy podejmując czynności w sposób zgodny z obowiązującymi zasadami nie naruszą żadnych regulacji procesowych, co mogłoby podważyć wiarygodność - a w konsekwencji jakąkolwiek moc prawną, pozyskiwanych dowodów.

Z punktu widzenia prawnego, szczególnie istotnym staje się rozstrzygnięcie kwestii granic dopuszczalności nakładania na osoby fizyczne obowiązku udostępniania, czy też ujawniania organom procesowym haseł lub kodów dostępowych, umożliwiających pozyskanie danych przetwarzanych lokalnie, bądź przetwarzanych też w usługach sieciowych. W przypadku bowiem, gdy czynność przeszukania wykonywana jest wobec osoby posiadającej status choćby osoby podejrzanej - a zatem osoby, której nie postawiono jeszcze żadnych zarzutów, osoba taka chroniona jest już na obecnym etapie postępowania zasadą *nemo se ipsum*, a więc nie może być zmuszana do udzielania jakiegokolwiek wsparcia organom procesowym. W szczególności też, nie powinna być przesłuchiwana w charakterze świadka. Instytucja świadka może natomiast stanowić swoiste rozwiązanie niełatwego problemu dostępu do danych zablokowanych, w przypadku gdy na świadka powołany zostanie np. administrator systemu, który nie pełni w procesie żadnej innej roli. W ramach składanych zeznań - które muszą być oczywiście prowadzone po należytym poinformowaniu świadka o możliwości uchylenia się od odpowiadania na wybrane lub wszystkie pytania - świadek może bowiem zostać zapytany o treść hasła lub innego kodu gwarantującego dostęp do określonej ilości danych. Uzyskanie przez organy procesowe hasła do usługi sieciowej realizowanej poza granicami kraju wydaje się jednak nie zmieniać zaprezentowanej wcześniej kwalifikacji

[73] A.Lach w: Dowody cyfrowe..., op. cit., s. 5-6.

prawnej działania w tym zakresie, jako wymagającego udziału procesowego organów państwa trzeciego w ramach stosowania pomocy prawnej. Problem ten pozostaje w ścisłym związku ze wskazanym wyżej brakiem zasad odnoszących się do procesu określania tzw. cyberjurysdykcji oraz wyznaczania dopuszczalnego zasięgu ingerencji organów poszczególnych państw w obszarze cyberprzestrzeni.

Z uwagi na ustawicznie rosnącą ilość danych, które przetwarzane są dzisiaj w szeroko rozumianych zasobach cyberprzestrzeni, prowadzenie przeszukań systemów teleinformatycznych napotyka także szereg problemów *stricte* technicznych, związanych jednak z koniecznością zapewnienia skuteczności, ale także ekonomiki działań procesowych, które nie mogą przecież ciągnąć się latami. Podczas, gdy zaledwie kilkanaście lat temu pobranie z sieci Internet pliku o rozmiarze zaledwie kilku megabajtów wymagało przynajmniej 5 minut czasu pobierania na przeciętnym domowym łączu sieciowym, dziś ten sam czas, przy zastosowaniu równie przeciętnego łącza internetowego, pozwala na ściągnięcie porcji danych nawet dwudziestokrotnie większej! Opisana sytuacja, powoduje iż dokonując przeszukań zawartości nawet prostych systemów teleinformatycznych, funkcjonariusze organów ścigania mogą stawać przed zadaniem o ogromnej skali, wymagającym setek godzin pracy celem ustalenia, czy badany materiał w ogóle zawiera materiał, który pozostaje w prawnie relewantnym związku z toczącym się postępowaniem karnym. Co także było sygnalizowane wyżej - przeszukiwane dane mogą występować w szeregu formatów, wymagając nierzadko wysoce specjalistycznej wiedzy dla dokonywania ich analiz procesowych lub też być zapisane na wielu połączonych nośnikach (np. w macierzach dyskowych, które mogą powodować, iż jeden plik zapisany jest w drobnych częściach pomiędzy kilkoma dyskami twardymi). W sytuacji takiej, celem zapewnienia poprawnego przebiegu procesu, ale także dla minimalizacji uciążliwości związanych z prowadzeniem przeszukania po stronie osób wobec których realizowana jest czynności, przeszukanie systemu może być dokonywane wobec kopii danych, które zostały uprzednio zabezpieczone w przeszukiwanym systemie w ramach wykonania tzw. czynności zatrzymania danych. Rozwiązanie to pozwala na fizyczne przeniesienie miejsce realizacji czynności przeszukania do pomieszczeń organów ścigania, pozwalając funkcjonariuszom na wykonywanie specjalistycznych czynności z zakresu informatyki śledczej, które nierzadko też wymagają dostępu do specjalistycznych narzędzi sprzętowo - programowych. Zgodnie z przyjętą konstrukcją rozdziału, problematyka zatrzymania danych została przybliżona w dalszej części opracowania. W tym miejscu, należy jedynie zauważyć, iż w przypadku konieczności zatrzymania danych, spowodowanej czy to rozmiarami woluminu

przeszukiwanych danych, cz też wystąpieniem braku woli współpracy z organami procesowymi, występującym po stronie dysponenta lub użytkownika systemu, ewentualnie realizowane zatrzymanie danych, winno odbywać się z zachowaniem wszelkich rygorów prawnych, którymi obwarowana została ta czynność w przepisach Kodeksu postępowania karnego (w szczególności przewidzianych w przepisie art. 227 Kodeksu postępowania karnego). Pośród najważniejszych z nich należy wskazać na obowiązek minimalizacji zakresu ingerencji w dobra prawnie chronione człowieka i obywatela.

Z przeprowadzenia czynności przeszukania systemu teleinformatycznego konieczne jest ostatecznie sporządzenie stosownego protokołu, w którym wskazane zostanie w sposób jednoznaczny jaki był zakres oraz sposób prowadzenia przeszukania. Z uwagi na specyfikę przeszukiwania danych komputerowych, protokół - oprócz podstawowych elementów opisanych w procedurze karnej, powinien zawierać skróty kryptograficzne zabezpieczonych materiałów, które będą mogły służyć za dowód, iż przetwarzane dalej materiały dowodowe nie zostały poddane nieuprawnionym modyfikacjom. Postulat ten dotyczy w szczególności zabezpieczania danych zaszyfrowanych, których treść w chwili realizacji przeszukania nie jest znana nie tylko przedstawicielom organów procesowych, ale z formalnego punktu widzenia, także innym osobom biorącym udział w czynności, o ile nie jest możliwe wykazanie im, iż uzyskiwały dostęp do zaszyfrowanych danych.

Kończąc rozważania szczegółowe na temat problematyki prawnej podejmowania czynności przeszukania wobec zasobów systemów teleinformatycznych, niezbędne jest także przybliżenie kwestii dokonywania takiego przeszukania na odległość, to jest za pośrednictwem sieci, bez fizycznego kontaktu z urządzeniem lub nośnikiem, którego cyfrowa pamięć staje się obszarem realizacji przedmiotowej czynności. Tak zwane przeszukanie na odległość może przybrać jedną z dwóch form[74], to jest:

1) przeszukania rozszerzonego; albo,
2) przeszukania zdalnego - rozumianego, jako przeszukanie wykonywane bez wymaganego udziału dysponenta lub użytkownika systemu.

Ideą przeszukania rozszerzonego, jest swoiste rozciągania zasięgu prowadzonego przeszukania, na zasoby systemu, który choć pierwotnie nie był objęty przeszukaniem, został włączony w jego zakres z uwagi na występujące pomiędzy systemami teleinformatycznymi połączenia. Przykładem takiego powiązania systemów może być choćby komputer funkcjonujący w tzw. sieci korporacyjnej. O ile komputer taki przetwarza określoną porcję

[74] Wyróżnione kategorie przytaczam za: A. Lach, Przeszukanie na odległość..., op. cit., s. 67 i nast.

danych lokalnie, o tyle może okazać się, iż istotna część wykonywanej na nim pracy zapisywana jest fizycznie na nośnikach zlokalizowanych np. w serwerowni danego podmiotu, który dbając o bezpieczeństwo danych, składuje je w jednym, ściśle chronionym miejscu. Celem rozszerzenia przeszukania systemu, jest zatem uzyskanie dostępu do zasobów, które przetwarzane są przy wykorzystaniu systemów połączonych z systemem pierwotnym.

Od przeszukania rozszerzonego należy odróżnić przeszukanie zdalne, które polega na uzyskaniu przez organy wymiaru sprawiedliwości dostępu do określonego systemu teleinformatycznego bez udziału jakichkolwiek osób trzecich - w tym nawet dysponenta lub użytkownika, często wręcz w sposób niejawny, ukryty przede wszystkim właśnie przed osobami posiadającymi uprawiony dostęp do zasobów systemu. Ów zdalny dostęp musi odbywać się z zastosowaniem narzędzi analogicznych do tych, którymi posługują się cyberprzestępcy podejmujący próby penetracji zabezpieczeń atakowanych elementów cyberprzestrzeni.

Od strony prawnej - należy w pierwszej kolejności zaznaczyć, iż żadna z poruszonych instytucji procesowych nie znajduje uregulowania w obowiązujących przepisach krajowego Kodeksu postępowania karnego, wymuszając w konsekwencji prowadzenie dalszej analizy prawnej wyłącznie w kontekście prawno-porównawczym.

Pierwsza z wymienionych czynności procesowych, to jest przeszukanie rozszerzone, zostało wprowadzone wprost w postanowieniach Konwencji Rady Europy o cyberprzestępczości[75], podpisanej w Budapeszcie jeszcze w 2001 r. Zgodnie z przepisem art. 19 ust. 2 Konwencji:

> „Każda Strona przyjmie środki prawne i inne, które mogą być potrzebne dla zapewnienia, aby właściwe organy dysponowały odpowiednimi środkami pozwalającymi na niezwłoczne rozszerzenie przeszukania lub podobnych metod uzyskiwania dostępu na inny system, jeżeli podczas dokonywania przez nie przeszukania lub uzyskiwania dostępu przy użyciu podobnych metod do konkretnego systemu informatycznego lub jego części, zgodnie z ustępem 1.a, organy te mają uzasadnione podstawy by sądzić, że poszukiwane dane przechowywane są w innym systemie informatycznym lub w jego części na ich terytorium i że do danych tych można legalnie uzyskać dostęp z systemu pierwotnego lub są one dostępne dla tego systemu."[76].

[75] Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[76] W oryginale „ *2. Each Party shall adopt such legislative and other measures as may be necessary to ensure*

Co wynika wprost z redakcji przytoczonego przepisu, strony Konwencji budapesztańskiej przesądziły o legalności rozszerzania zakresu przeszukań zasobów systemów teleinformatycznych na tzw. systemy powiązane, do których uzyskuje się dostęp z systemu pierwotnego.

W świetle brzmienia, jakie ostatecznie przyjęła redakcja art. 19 ust. 2 Konwencji, zasadne staje się natomiast postawienie pytania o dopuszczalny zakres rozszerzania przeszukań w kontekście cyberjurysdykcyjnym - innymi słowy, czy przepis ten należy rozumieć, jako wyznaczający swoiste minimum, czy też maksimum *cyberprzestrzennych* uprawnień organów procesowych państw-stron Konwencji? Nakreślony problem można zaprezentować przy zastosowaniu dwóch, następujących hipotez badawczych:

1) przepis art. 19 ust. 2 Konwencji wyznacza dopuszczalny zakres prowadzenia przeszukania rozszerzonego systemów teleinformatycznych, wyznaczając jego zasięg w obrębie zasobów systemów, które znajdują się fizycznie na terytorium jednego państwa; lub też,
2) przepis art. 19 ust. 2 wyznacza jedynie wspólne minimum uprawnień procesowych państw-stron Konwencji, gwarantując organom krajowym prowadzącym przeszukania systemów dostęp do tzw. systemów powiązanych.

Za pierwszą z przedstawionych wyżej interpretacji wydają się przemawiać zasady wykładni językowej przepisów (w szczególności stosowanie rozumowania *a contrario*), uzupełniane w sposób istotny wyjaśnieniem zawartym w punkcie 193 Raportu Wyjaśniającego do Konwencji[77]. Punkt ten stanowi w nieco innej konstrukcji językowej, że system lub jego część, na które rozszerzany jest zakres przeszukania „musi także znajdować się na terytorium tego państwa”[78]. Za przyjęciem interpretacji drugiej, należy natomiast opowiedzieć się stosując zasady wykładni systemowej - które nakazują w analizowanym przypadku uznać, że zakres przedmiotowy komentowanego przepisu skupia się wyłącznie na środkach podejmowanych na poziomie krajowym, a więc *ex definitione* przepis ten nie powinien

that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.” Tłumaczenie pochodzi z oficjalnego przekładu Konwencji, Dz. U. z 2015 r., poz. 728.

[77] *Explanatory Report*, pełen tekst dokumentu dostępny jest na stronie internetowej pod adresem: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[78] W oryginale: „ 193. Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be 'in its territory'.”. Tłumaczenie własne.

w ogóle poruszać tematyki związanej z zagadnieniami cyberjurysdykcji międzynarodowej, pozostawiając ją tym samym poza zakresem swojego meritum regulacyjnego.

W powyższym kontekście równie istotne, co problematyczne staje się także ustalenie poprawnego rozumienia zastosowanego w przepisie zwrotu „dane prawnie dostępne lub możliwe do przetwarzania z systemu pierwotnego", stanowiącego swoistą próbę logicznego powiązania zasobów teleinformatycznych systemów: przeszukiwanego oraz powiązanego (na obszar którego rozszerzane będzie przeszukanie). Mając na uwadze, iż znakomita większość systemów sieciowych podłączona jest obecnie do sieci rozległej Internet, można zaryzykować stwierdzenie, iż z punktu widzenia technicznego, uzyskując w ramach czynności przeszukania, dostęp do zasobów systemu, który tylko podłączony jest do sieci globalnej - potencjalnie, za jego pośrednictwem uzyskuje się dostęp do wszelkich zasobów cyberprzestrzeni. Interpretacja ta prowadzi w istocie do wniosku, iż tak określone rozszerzenie przeszukania w istocie nie posiada żadnych granic, o ile tylko dostęp będzie nosił znamię „prawności". Rozwiązanie takie z pewnością nie było jednak intencją autorów komentowanej regulacji prawnej. Jej znaczenie należy zatem rozumieć w kontekście ściślejszych powiązań systemowych, opierających się na konieczności łączenia zasobów systemów dla umożliwienia realizacji ich funkcji (np. dostęp do serwera pocztowego, czy też wirtualnego dysku, na którym faktycznie przechowywane są dane przetwarzane na przeszukiwanej stacji klienckiej), co nie znajduje jednak jednoznacznego oparcia w przyjętej redakcji przepisu.

W ocenie autora niniejszej pracy, swoistego rozwiązania prezentowanych wątpliwości prawnej, należy poszukiwać pośród aspektów technicznych realizowania czynności przeszukania systemu teleinformatycznego. Mając bowiem na uwadze kwestie związane z lokalizowaniem informatycznych nośników danych, na których fizycznie znajdują się przeszukiwane materiały - należy ponowić wyrażony wcześniej pogląd, iż o ile określone materiały, które pierwotnie zapisane są np. na dysku sieciowym firmy *Google,* znajdującym się w serwerowni w USA, czy też Finlandii, zostaną dobrowolnie pobrane przez ich uprawnionego użytkownika („uprawnionego" w sensie technicznym) oraz udostępnione organom ścigania jako dane występujące już na systemie tegoż użytkownika zlokalizowanym na terenie kraju - tak realizowana czynność przeszukania będzie ograniczać się do „systemów lub ich części znajdujących się na terytorium jednego państwa". Bez znaczenia prawnego pozostawać bowiem będzie w tym miejscu fakt, że pobrane dane występują w badanym systemie choćby wyłącznie w formie zapisu ulotnego, skoro fizyczne odcięcie tego systemu od sieci nie będzie już ograniczać możliwości wykonania czynności procesowej

w odniesieniu do określonej porcji danych. Brak natomiast współpracy ze strony podmiotu wzywanego do wydania określonych danych komputerowych zapisanych na nośnikach „zagranicznych" oznaczać będzie w tej sytuacji konieczność uzyskania wsparcia międzynarodowego w tym zakresie, w ramach stosowania pomocy prawnej.

Wskazując przykłady krajowych regulacji procesowych przewidujących możliwość prowadzenia przeszukania rozszerzonego systemów teleinformatycznych, przywołać należy w szczególności rozwiązania francuskie, brytyjskie, belgijskie oraz holenderskie[79]. Zgodnie z przepisem art. 57-1 francuskiego kodeksu postępowania karnego z 1958 r., przeszukanie zasobów systemu informatycznego znajdującego się w miejscu realizacji czynności może zostać rozszerzone na zasoby innego systemu, do którego możliwe jest uzyskanie dostępu z systemu przeszukiwanego. O ile jednak system powiązany zlokalizowany jest poza granicami Francji, uzyskanie dostępu do jego zasobów wymaga zastosowania instytucji pomocy prawnej. Podobnie z punktu widzenia praktycznego - zgodnie z przepisem art. 19 (4) brytyjskiej ustawy *Police and Criminal Evidence Act* z 1984 r., dokonując przeszukania pomieszczeń, konstabl realizujący czynności ma prawo uzyskiwania wglądu do każdej informacji, która tylko dostępna jest z przeszukiwanego pomieszczenia, co jest aktualnie odczytywane jako prawo do rozszerzania zakresu przeszukania na systemy teleinformatyczne zlokalizowane w tym pomieszczeniu oraz systemy powiązane. Nieco bardziej rozbudowana regulacja prawna instytucji przeszukania rozszerzonego w kontekście systemów teleinformatycznych zawarta została w prawie belgijskim. Jak stanowi art. 88ter belgijskiego kodeksu postępowania karnego, przeszukanie systemu teleinformatycznego lub jego części, może zostać rozszerzone na inne systemy lub ich części, które mogą być lokalizowane poza miejscem realizacji czynności. Rozszerzenie takie możliwe jest jednak po spełnieniu określonych w ustawie przesłanek, takich jak występowanie prawnie relewantnego związku pomiędzy rozszerzeniem przeszukania a przestępstwem, w związku z którym czynność ta jest realizowana w systemie pierwotnym, ryzyko utraty dowodów występujących w systemie powiązanych, czy też wreszcie konieczność zapewnienia proporcjonalności działań organów państwowych. Obwarowane takimi wymogami rozszerzenie może dotyczyć systemów, do których dostęp mają osoby upoważnione do użytkowania systemu pierwotnego. Co istotne - w przypadku ustalenia, że dane uzyskiwane w ramach rozszerzenia przeszukania zlokalizowane są poza granicami kraju, dane takie podlegają skopiowaniu o czym informuje się, za pośrednictwem Ministra

[79] Przykłady przytaczam za: A. Lach, Przeszukanie na odległość..., op. cit., s. 69 i nast.

Sprawiedliwości, państwo na terytorium którego dane te są przechowywane fizycznie. Ostatecznie, ciekawym przykładem regulacji dopuszczającej rozszerzenie przeszukania na systemy teleinformatyczne powiązane z systemem pierwotnym, jest także przepis art. 125j holenderskiego kodeksu postępowania karnego, dopuszczający wprowadzenie takiego rozszerzenia w stosunku do danych zlokalizowanych gdziekolwiek oraz uprawniający do wykonania ich kopii. Co istotne - zakres rozszerzanego dostępu nie może być szerszy, niż zakres dostępu osób mieszkających lub zwykle pracujących, czy też przebywających w pomieszczeniu objętym czynnością przeszukania.

Powracając na grunt krajowy, należy ostatecznie zauważyć, iż Polski Kodeks postępowania karnego nie przewiduje w obecnym brzmieniu możliwości prowadzenia przeszukania rozszerzonego systemów teleinformatycznych, stawiając jednocześnie wymogi prawne, które wydają się wręcz wykluczać możliwość realizacji takiej czynności. W szczególności należy bowiem wskazać, iż przeszukanie systemu innego niż objęty postanowieniem może wymagać uprzedniego wezwania jego dysponenta lub użytkownika (w sytuacji braku współpracy ze strony użytkownika systemu pierwotnego) do wydania określonych danych oraz wiąże się z koniecznością zapewnienia tej osobie możliwości faktycznego udziału w realizowanej czynności - co razem będzie najczęściej wiązało się z koniecznością fizycznego udania się przedstawicieli organu procesowego do miejsca, gdzie przetwarzane są dane komputerowe poddawane czynności przeszukania.

Od instytucji procesowej przeszukania rozszerzonego należy natomiast odróżnić z całą stanowczością konstrukcję prawną tzw. przeszukania na odległość, wywołującego szereg kontrowersji zarysowujących się na tle ochrony praw człowieka i obywatela przed nadmierną ingerencją ze strony organów państwowych. Istotą czynności procesowej nazywanej „przeszukaniem na odległość" jest bowiem uzyskanie dostępu do zasobów systemu teleinformatycznego bez udziału osób innych niż sami funkcjonariusze, w szczególności zaś bez udziału jego użytkownika, dysponenta, czy też właściciela. Z uwagi na stosowane dziś powszechnie zabezpieczenia dostępu do danych komputerowych (choćby wbudowane w systemy operacyjne, jako jedne z ich podstawowych funkcjonalności), dostęp taki najczęściej musi wiązać się z koniecznością przełamania owych zabezpieczeń przez organy procesowe w ramach wykonywania czynności analogicznych (o ile nie wręcz identycznych) w swojej metodyce, do prowadzenia cyberataków, typizowanych przecież jako przestępstwa w rozumieniu przepisów karnych. Mając powyższe na uwadze, legalizowanie czynności przeszukania zdalnego musi zatem wiązać się z wprowadzeniem do krajowych porządków prawnych rozbudowanych kontratypów, wyłączających bezprawność opisywanych działań

w przypadku ich realizacji przez organy państwowe. Regulacje takie zarysowują oczywiście istotny wyłom w zasadach ochrony podstawowych praw i wolności człowieka i obywatela przed nieuzasadnioną ingerencją władz państwowych. Zarzut ten, w przypadku prowadzenia zdalnych przeszukań szeroko rozumianych zasobów cyberprzestrzeni, dodatkowo ogniskowany jest przez fakt, iż przeszukania takie zachowują swój podstawowy sens w przypadku realizacji czynności przeszukania w sposób niejawny, to jest z wyłączeniem informowania o tym fakcie użytkowników, dysponentów lub właścicieli systemu.

Najgłośniejszym przykładem działań organów państwowych w zakresie wdrożenia przeszukań zdalnych, stały się starania władz niemieckich, które nie tylko podjęły próbę wprowadzenia stosownych regulacji prawnych na szczeblu landów, ale także przygotowały specjalistyczne narzędzia programistyczne do włamywania się do zasobów przeszukiwanych komputerów, ochrzczone później w prasie światowej mianem *bundes-trojaner* lub też *staats-trojaner*[80], czyli państwowymi trojanami[81]. Na marginesie warto zaznaczyć - co stanowi swoistą ironię losu, iż istnienie niemieckich trojanów państwowych zostało wykryte przez grupę hackerską CCC, która w trakcie realizacji swoich włamań zwróciła uwagę na osobliwe fragmenty kodu złośliwego, przypisanego później firmie powiązanej z kontraktem rządowym. Uchwalona w końcu 2006 r. w Nadrenii-Westfalii ustawa o ochronie konstytucji wprowadziła do niemieckiego porządku prawnego instytucję tajnego, realizowanego na odległość przeszukania zasobów systemu teleinformatycznego. Regulacja ta stała się swoistą odpowiedzią na negatywne stanowisko sądów niemieckich w zakresie dopuszczalności uzyskiwania dostępu do zasobów systemów teleinformatycznych w oparciu o przepisy konstytuujące zasady prowadzenia podsłuchu. Po licznych kontrowersjach oraz fali sprzeciwów pojawiających się na tle znaleziska grupy CCC - podsycanych dodatkowo faktem, iż państwowe oprogramowanie szpiegowskie zostało przecież sfinansowane z pieniędzy samych podatników, niemiecki trybunał konstytucyjny orzekł w początku 2008 r. o niekonstytucyjności przywołanych regulacji, wskazując w szczególności na nieproporcjonalność zaproponowanego środka. Trybunał wskazał bowiem między innymi, iż w odróżnieniu od typowego podsłuchu, przeszukanie zdalne umożliwia dostęp do wszystkich zasobów użytkowników systemów, które to zasoby obejmują w dzisiejszych czasach liczne dane o charakterze wręcz intymnym, jeśli nie tylko prywatnym. Co jednak znamienne,

[80] Więcej na temat wskazanego oprogramowania można znaleźć na stronie internetowej dostępnej pod adresem: http://en.wikipedia.org/wiki/Chaos_Computer_Club#Staatstrojaner.

[81] Trojan w technicznym slangu teleinformatycznym to rodzaj oprogramowania szpiegującego, które pozwala przeniknąć do zasobów atakowanego systemu niczym mitologiczny Koń Trojański, by następnie wykonać szereg zadanych przez jego dysponenta operacji.

trybunał federalny nie podważył legalności instytucji przeszukania zdalnego *in abstracto,* lecz przyjęty sposób jej implementacji[82]. Na tle tak sformułowanego wyroku, niespełna rok później - to jest w dniu 1 stycznia 2009 r., do niemieckiej ustawy regulującej uprawnienia służb kryminalnych *Bundeskriminalamtgesetz*[83], wprowadzony został przepis § 20k (*Verdeckter Eingriff in informationstechnische Systeme*), zezwalający na prowadzenie zdalnych przeszukań *on-line* przez organy policyjne, o ile zachodzi uzasadnione podejrzenie wystąpienia najistotniejszych zagrożeń dla ludzkiego życia, wolności lub też podstaw egzystencji państwa niemieckiego.

Swoistym przykładem rozwiązań organizacyjno-technicznych mających na celu umożliwienie realizacji wybranych elementów czynności przeszukania zdalnego, stał się w ostatnich czasach także amerykański, rządowy program funkcjonujący pod nazwą PRISM. Zgodnie z doniesieniami prasowymi, ujawniony przez byłego funkcjonariusza CIA program, ma zapewniać służbom amerykańskim dostęp *on-line* do zasobów teleinformatycznych przetwarzanych przez wybranych dostawców usług sieciowych, którzy zostali włączeni w zakres programu za pomocą tajnych porozumień. Pośród dostawców takich wskazywany był m.in. koncern *Google*, który miał zapewniać dostęp do kont poczty elektronicznej funkcjonujących w usłudze *Gmail*. Wszelkie informacje na temat programu posiadają jednak wyłącznie medialny charakter, nie pozwalając tym samym na prowadzenie ich rzetelnej analizy prawnej.

Na gruncie przepisów Polskiego kodeksu postępowania karnego realizowanie czynności zdalnego przeszukania nie tylko znajduje żadnego oparcia, ale stanowi wręcz naruszenie szeregu zasad procesowych, jak choćby gwarancji udziału osób objętych przeszukaniem w prowadzonej czynności. Co więcej - żadna z tzw. ustaw policyjnych, jak również sam Kodeks karny, nie przewidują w obecnym brzmieniu stosownych uprawnień oraz skorelowanych z nimi kontratypów, które dopuszczałyby podejmowanie przez służby krajowe czynności zdalnego przeszukania dowolnych zasobów cyberprzestrzeni[84].

---

82 Powtarzam za: A. Lach, Przeszukanie na odległość..., op. cit., s. 69 i nast.

83 Pełny tekst ustawy w języku niemieckim dostępny jest na stronie internetowej pod adresem: http://www.gesetze-im-internet.de/bkag_1997/BJNR165010997.html.

84 Na konieczność wprowadzenia stosownych regulacji wskazuje A. Adamski w: Przestępczość w cyberprzestrzeni..., op. cit., s. 129.

2. Problematyka karno-procesowa prowadzenia czynności zatrzymania danych w cyberprzestrzeni

Zatrzymanie danych - będące w istocie odmianą instytucji zatrzymania rzeczy, stanowi jeden z podstawowych środków służących utrwaleniu dowodów popełnienia cyberprzestępstwa. Analogicznie, jak konwencjonalne zatrzymanie rzeczy *fizycznych*, czynność ta stanowi w efekcie narzędzie zabezpieczające poprawny przebieg postępowania karnego, szczególnie w kontekście prowadzonego w jego ramach postępowania dowodowego.

Z uwagi na specyfikę cyberprzestrzeni, stanowiącej obszar wyłącznie logiczny (wirtualny), wyznaczany granicami o ponad-geograficznym charakterze, szeroko rozumiane dane komputerowe niejako wymykają się typowym regulacjom przewidzianym dla zatrzymywania rzeczy, prezentując szczególną problematykę obcowania z nienamacalnymi bitami, zapisanymi w postaci impulsów elektromagnetycznych. Stwierdzenie to skłania do postawienia tezy, iż poprawne zrozumienie instytucji zatrzymania danych wymaga jej umiejscowienia w środowisku naturalnym danych oraz kontekście praktycznym.

Rozpoczynając analizę merytoryczną zagadnienia zatrzymywania danych należy w pierwszej kolejności zaznaczyć, iż czynność ta może być realizowana bądź to poprzez fizyczny kontakt z informatycznym nośnikiem danych, na którym zapisane są pliki bądź też inne materiały podlegające zatrzymaniu, lub też za pośrednictwem sieci (to jest *on-line*) czyli z wykorzystaniem cyberprzestrzeni. Z pierwszą ze wskazanych sytuacji mamy do czynienia np. w ramach uzyskiwania przez funkcjonariuszy fizycznego dostępu do komputera, na którym zlokalizowane są zatrzymywane dane. Z drugą - choćby w momencie wykonywania kopii strony internetowej, której pliki zapisane są fizycznie na serwerze zlokalizowanym w dowolnym punkcie na świecie, innym niż komputer służący do otwarcia oraz „zgrania" strony.

Niezależnie od przyjętej drogi dostępu do zatrzymywanych danych komputerowych, wskazana czynność polega w istocie na wykonaniu kopii danych stanowiących materiał dowodowy. Z uwagi na zasady funkcjonowania informatycznych nośników danych, nawet przeniesienie danych sprowadza się w rzeczywistości technicznej do wykonania ich kopii wraz z jednoczesnym usunięciem zapisu oryginalnego. Innymi słowy - dane komputerowe poddane kopiowaniu nie wędrują pomiędzy nośnikami, zmieniając w sposób trwały swoje umiejscowienie, zaś są odczytywane na nośniku źródłowym, wysyłane za pośrednictwem systemu do właściwego sterownika nośnika docelowego oraz ostatecznie, zapisywane na tym drugim w postaci stosownego zapisu elektromagnetycznego (dyski twarde, pamięci *flash* typu *pendrive*) lub optycznego (płyty CD, DVD, Blu-ray). Fizyczne zatrzymanie samego nośnika

danych - stanowiące w istocie przejaw zatrzymania rzeczy, pozostawiane jest poza zakresem prowadzonej w tym miejscu analizy prawnej, jako niewymagające szczególnego traktowania w ujęciu zasad przetwarzania zasobów cyberprzestrzeni.

Mając na uwadze wcześniejsze rozważania na temat uznawania wartości dowodowej kopii danych - zawarte w części ogólnej rozdziału oraz poczynione przy okazji analizy problematyki przeszukania zasobów cyberprzestrzeni, w tym miejscu podkreślenia wymagają następujące kwestie:

- dane w postaci cyfrowej poddają się nie tyle bezstratnemu powielaniu, co wykonywaniu wprost identycznych kopii, zachowujących wszelkie cechy oryginału,
- kopie elektronicznych dokumentów lub też innych materiałów, opatrzonych tzw. podpisem elektronicznym, zachowują nie tylko tożsamość treściową, ale także swój walor autentyczności, obejmując kopią nie tylko zawartość, ale także dane składające się na podpis. Kopia dokumentu elektronicznego opatrzona stosownym podpisem cyfrowym nie poddaje się w konsekwencji traktowaniu analogicznemu, jak np. ksero dokumentu, na którym umieszczony był podpis odręczny - choć głosy takie można znaleźć w piśmiennictwie[85] - zaś stanowi równorzędny materiał,
- pliki komputerowe, obok danych składających się na ich treść, zawierają także metadane (*dane o danych*) opisujące określone atrybuty plików, jak np. datę ich utworzenia, datę ostatniej modyfikacji, imię autora itd. Zapewnienie pełnej jednolitości pliku źródłowego oraz jego kopii, wymaga w konsekwencji zadbania o zbieżność całego zestawu danych budujących ten plik, to jest z uwzględnieniem metadanych. Ponieważ podstawowe funkcje systemów operacyjnych (jak choćby znana z rodziny Windows funkcjonalność „przeciągania” ikon plików pomiędzy oknami, symbolizującymi z kolei katalogi) prowadzą do modyfikacji metadanych, wykonywanie procesowych kopii danych wymaga stosowania specjalistycznych narzędzi programowo-sprzętowych, nazywanych blokerami, służących do zapewnienia pełnej zbieżności materiału skopiowanego z oryginałem,
- techniczną metodą porównywania identyczności plików komputerowych (lub też dowolnych innych porcji danych, nazywanych czasami *blobami*) jest wykonywanie tzw. skrótów kryptograficznych, stanowiących swoisty odcisk linii papilarnych pliku. W języku technicznym, odciski takie określane są anglojęzycznym określeniem *hash*.

---

85 Tak np. M. Zelek, op. cit.

Z uwagi na zastosowane w funkcjach skrótu skomplikowane rozwiązania kryptograficzne, szansa wygenerowania dwóch identycznych skrótów (odcisków) z różnych plików wyrażana jest liczbą 2^{160} lub większą, w zależności od zastosowanej funkcji kryptograficznej[86]. Potwierdzenie oryginalności pliku polega w konsekwencji na wykonaniu skrótu z pliku zabezpieczanego oraz późniejszym, ponownym wykonaniu skrótu z pliku wykorzystywanego, jako materiał dowodowy. W przypadku zbieżności obydwu skrótów, potwierdzony zostaje fakt nienaruszenia integralności zabezpieczonego materiału,

- z uwagi na konieczność zapewnienia autentyczności danych odnajdywanych w ramach wykonywania czynności procesowego przeszukania zasobów systemu teleinformatycznego, wykonywanie kopii danych stanowi nierzadko pierwszy element realizacji takiego przeszukania. Dalsze czynności przeszukania podejmowane są w tej sytuacji już w odniesieniu do danych skopiowanych, co wyklucza możliwość wprowadzenia nieumyślnych modyfikacji w danych oryginalnych, ale także istotnie zmniejsza uciążliwość związaną z realizacją czynności, występującą po stronie dysponenta badanych nośników. Wykonywanie kopii danych stanowi wręcz nieodzowny element przeszukiwania dużych woluminów danych, co z uwagi na wysoką czasochłonność, musi być wykonywane w obiektach organu procesowego. Wspomniane wcześniej modyfikacje przeszukiwanych danych stanowią o konieczności unieważnienia pozyskanego materiału dowodowego, który jako zmieniony, traci walor autentyczności oraz wiarygodność procesową,
- wykonywanie kopii danych może ostatecznie stanowić jedyny sposób utrwalenia danych, przetwarzanych wyłącznie w postaci zapisu ulotnego, występującego np. w pamięci operacyjnej komputera (RAM). Z sytuacją taką mamy do czynienia choćby w przypadku utrwalenia pliku - dokumentu elektronicznego, który nie został jeszcze zapisany przez użytkownika komputera na dysku, natomiast jest już przetwarzany w edytorze dokumentów, lub też dopiero sporządzanej, choć jeszcze nie wysłanej, wiadomości poczty elektronicznej.

O ile jednak zatrzymanie danych realizowane przy zachowaniu bezpośredniego dostępu funkcjonariuszy do nośników, na których zapisane są materiały podlegające utrwaleniu dowodowemu - nie wydaje się nastręczać istotnych problemów prawnych, o tyle

[86] Więcej na temat funkcji skrótu na stronie internetowej dostępnej pod adresem: http://pl.wikipedia.org/wiki/Funkcja_skr%C3%B3tu.

ocena ta podlega zasadniczemu przewartościowaniu w przypadku realizacji czynności zatrzymania za pośrednictwem cyberprzestrzeni, a więc zdalnie, czy też na odległość. Sytuacja taka może zachodzić w dwóch konfiguracjach faktycznych: po pierwsze, w toku realizacji zdalnego przeszukania; po drugie zaś - w ramach zatrzymania materiałów dostępnych publicznie dla dowolnego użytkownika sieci lub też grupy użytkowników spełniających określone wymogi (np. posiadających zarejestrowane konta w określonej usłudze sieciowej). Ponieważ sytuacja pierwsza, pozostająca w ścisłym związku z problematyką prowadzenia czynności przeszukania zdalnego, stanowiła przedmiot pogłębionych rozważań prowadzonych na gruncie poprzedniej części rozdziału - niniejsze rozważania szczegółowe zostają ograniczone do analizy sytuacji drugiej. Podkreślenia w tym miejscu wymaga jednak fakt, iż z punktu widzenia karnoprocesowego, instytucja zatrzymania rzeczy pozostaje w swoich ramach prawnych zbieżna w obydwu wyszczególnionych sytuacjach, poddając się rozróżnieniu głównie w kontekście niejawnego charakteru realizacji przeszukania zdalnego.

Z konstrukcją klasycznego zatrzymania danych za pośrednictwem sieci mamy do czynienia w szeregu następujących, choć wyliczonych jedynie przykładowo sytuacji:

- wykonywanie kopii stron WWW zawierających treści o charakterze przestępnym, jak choćby materiały pornograficzne z udziałem osób nieletnich,
- pobieranie udostępnianych w Internecie plików zawierających treści bezprawne, nielegalne kopie oprogramowania, materiały nawołujące do popełnienia przestępstwa, informacje o sposobie przygotowania narzędzi zbrodni itd. Materiały takie mogą być uzyskiwane nie tylko ze stron internetowych, ale także bezpośrednio od innych użytkowników sieci, korzystających z tzw. rozwiązań *peer-to-peer*, jak popularna kiedyś *Kazaa*, czy też sieci *torrent*,
- wykonywanie kopii wpisów, tzw. *postów*, występujących na forach internetowych, grupach dyskusyjnych, tzw. *bulletin boards*, czy innych, analogicznych rozwiązaniach technicznych,
- wykonywanie tzw. zrzutów ekranu, czyli swoistych zdjęć zawartości wyświetlającej się na ekranie komputera, na których dostrzec można np. treść wpisów pojawiających się na czatach lub innych kanałach bieżącej komunikacji sieciowej, czy też,
- pozyskiwanie danych o ruchu sieciowym, wskazujących np. na listę adresów IP wykonujących połączenie z zaatakowaną usługą sieciową, gromadzonych w tzw. logach sieciowych. Dane takie mogą być pobierane zarówno od osób

dysponujących systemami, które stały się przedmiotem ataku, jak również od operatorów telekomunikacyjnych, na których nałożone są szczególne obowiązki prawne w ramach procedury tzw. retencji danych (opisane na gruncie regulacji krajowych w dalszej części rozdziału).

Powyższa typologia zatrzymania danych na odległość pozwala scharakteryzować opisywaną czynność, jako działanie:

1) podejmowane jednostronnie przez organy procesowe, to jest z wyłączeniem czynnego udziału osób faktycznie dysponujących zatrzymywanymi danymi. W przypadku zatrzymywania danych dokonywanego w ramach ich pobierania bezpośrednio od innego użytkownika sieci, jednostronność działania organu procesowego wyraża się przede wszystkim w braku świadomości po stronie osoby udostępniającej określoną porcję danych, iż uczestniczy w czynności zatrzymania;
2) realizowane *de facto* w sposób niejawny, w rozumieniu pominięcia obowiązków informacyjnych, czy też uprzedniego wezwania osoby do wydania rzeczy;
3) związane - w ujęciu technicznym, z uzyskaniem przez organ procesowy dostępu do zatrzymywanych danych z pozycji zwykłego użytkownika sieci, w tym użytkownika określonej usługi sieciowej (np. portalu WWW, na którym zamieszczone są nielegalne pliki);
4) obejmujące swoim potencjalnym zasięgiem całą cyberprzestrzeń, a zatem zasoby zlokalizowane fizycznie tak w kraju organu realizującego czynność, jak i dowolnym innym miejscu. Cecha ta powoduje szereg problemów związanych z zagadnieniem cyberjurysdykcji, mogąc wywołać potencjalną kolizję z normami prawnymi regulującymi instytucję pomocy prawnej.

Powyższe cechy powodują, iż *de iure* czynność zatrzymywania danych na odległość w istocie trudno jest określać mianem czynności procesowej w ujęciu klasycznym[87]. Ocena ta musi rzecz jasna wywierać istotny wpływ na możliwość zastosowania danych pozyskanych w toku zatrzymania na odległość, jako materiału dowodowego w postępowaniu karnym. W przypadku braku szczególnych regulacji prawnych, które dopuszczałyby w sposób wyraźny przyjęcie takiego materiału za dowód, należy opowiedzieć się za koniecznością przeprowadzenia procesowej waloryzacji opisywanych materiałów dokonywanej np. poprzez

[87] Ujęcie prezentowane np. w: T. Grzegorczyk, J. Tylman, Polskie postępowanie karne, Lexis Nexis, Warszawa 2011, wyd. 8, s. 552 i nast.

przesłuchanie w charakterze świadka osoby funkcjonariusza realizującego czynność[88]. Prowadzenie dalszej analizy w tym zakresie, wymaga jednak przeniesienia na grunt konkretnych regulacji prawnych.

W ujęciu prawno-porównawczym, zatrzymanie danych zostało opisane w szczególności na gruncie wielokrotnie przywoływanej w niniejszej pracy Konwencji o cyberprzestępczości[89]. Zgodnie z przepisem art. 19 ust. 3 Konwencji:

> „Każda Strona przyjmie środki prawne lub inne, które mogą być potrzebne dla nadania właściwym organom uprawnień do tego, aby mogły zajmować lub zabezpieczać w podobny sposób dane informatyczne, do których uzyskano dostęp zgodnie z ustępami 1 i 2 [regulującymi odpowiednio przybliżone wcześniej czynności: przeszukania oraz przeszukania rozszerzonego - kom. autora]. Środki te obejmują następujące uprawnienia:
>
> a zajęcie lub zabezpieczenie w podobny sposób systemu informatycznego lub jego części lub nośnika służącego do przechowywania danych informatycznych;
>
> b wykonywanie i zachowywanie kopii tych danych informatycznych;
>
> c zachowywanie całości odpowiednich przechowywanych danych informatycznych;
>
> d uczynienie niedostępnymi lub usunięcie danych informatycznych z danego systemu informatycznego."[90].

Komentując przywołany przepis, w pierwszej kolejności należy podkreślić, iż jego postanowienia zostały odniesione do trzech elementów przedmiotowych: systemów, ich części oraz szeroko rozumianych komputerowych nośników danych. Przyjęte brzmienie przepisu nadaje regulacji nieco konwencjonalnego zabarwienia, niejako sugerując, iż jego konstrukcja obejmuje w istocie klasyczne zatrzymanie („zajęcie") rzeczy - tyle, że odnoszone do zatrzymywania fizycznych elementów systemów teleinformatycznych. Dalsza część przepisu wprowadza jednak uściślenie postanowień zawartych we wstępie do wyliczenia,

---

88 A. Taracha, op. cit., s. 221 i nast. s. 225 i nast.

89 Pełny tekst konwencji dostępny na oficjalnej stronie internetowej Rady Europy pod adresem: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

90 W oryginale: *„3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system.*" Tłumaczenie pochodzi z oficjalnego przekładu wykonanego na potrzeby ratyfikacji Konwencji, Dz. U. z 2015 r., poz. 728.

wskazując iż zatrzymanie może być realizowane poprzez zarówno typowe zatrzymanie rzeczy (systemów oraz nośników) lub wykonanie kopii danych istotnych z punktu widzenia zabezpieczenia poprawnego przebiegu postępowania karnego. Jednocześnie, komentowany przepis wprowadza dwa dodatkowe, uzupełniające uprawnienia o charakterze technicznym oraz techniczno-organizacyjnym, zezwalające uprawnionym podmioty na zastosowanie rozwiązań teleinformatycznych służących do zapewnienia identyczności („*integrity*") wykonywanych kopii danych oraz *de facto* wyłączenie systemu poddanego czynności z jego dalszego użytku w celu zapewnienia nienaruszalności zgromadzonego na nim materiału. Wydaje się, iż ostatnie z wymienionych uprawnień ma na celu - obok wyłączenia dostępności danych o charakterze bezprawnym, także zagwarantowanie ochrony danych przed ich nieuprawnionymi modyfikacjami w przypadkach, gdy funkcjonariusze realizujący czynność nie są w stanie (choćby z powodu braku niezbędnych kwalifikacji) przeprowadzić czynności zatrzymania nośników lub danych. Co istotne, na gruncie przytoczonego postanowienia Konwencji, kwestia zatrzymywania danych została ściśle powiązana z zagadnieniem wykonywania kopii danych, wskazując - iż obok fizycznego zatrzymania nośników, jest to podstawowy sposób zatrzymywania danych komputerowych. Ponieważ do komentowanego przepisu zostało wprowadzone odesłanie do postanowień przepisu art. 19 ust. 1 i 2 Konwencji, należy zaznaczyć, iż opisana w tym miejscu czynność zatrzymania danych została ściśle powiązana z metodyką prowadzenia przeszukania systemu oraz tzw. przeszukania rozszerzonego - zakreślając tym samym legalny zasięg zatrzymania danych. W szczególności muszą to być dane zlokalizowane w systemie teleinformatycznym umiejscowionym w granicach kraju, którego organy podejmują się realizacji czynności. Opisany wyżej standard prawny, wyrażony postanowieniami Konwencji, wyznaczył ramy prawne zatrzymania danych dla większości państw europejskich, będących stronami konwencji budapesztańskiej.

Szczególnych regulacji odnoszących się do zatrzymywania danych należy szukać także w prawie amerykańskim. Przykładowo, zgodnie z paragrafem 2703 *U.S. Code*[91] (stanowiącego w istocie zbiór wszystkich regulacji prawnych, niczym krajowy Dziennik Ustaw), uprawnione organy mogą zatrzymywać dane stanowiące treści komunikatów elektronicznych bez uzyskiwania nakazu sądowego, o ile tylko przedmiotowe dane były przechowywane w systemach przedsiębiorców telekomunikacyjnych przez okres dłuższy niż 180 dni. Owa granica czasowa - wprowadzona do systemu prawa amerykańskiego jeszcze

[91] Tytuł 18, część I, rozdział 121, par. 2703 U.S. Code. Tekst jednostki dostępny na stronie internetowej pod adresem: http://www.law.cornell.edu/uscode/text/18/2703.

w 1986 r., w ustawie zatytułowanej w oryginale *Electronic Communications Privacy Act* (w wolnym tłumaczeniu - ustawa o prywatności komunikatów przekazywanych drogą elektroniczną) oraz jej swoistego uzupełnienia - ustawie *Stored Communications Act* (ustawa o przechowywaniu komunikatów), stanowi dziś jeden z podstawowych celów krytyki obrońców praw człowieka i obywatela w odniesieniu do ochrony poufności zasobów Internetu przed zakusami organów państwowych[92].

Zgodnie z ogólnymi regulacjami prawa amerykańskiego - zarysowującymi się w szczególności na tle czwartej poprawki do konstytucji, formułującej zasadę tzw. uzasadnionego oczekiwania prywatności[93], granica prywatności obywateli, tak w życiu codziennym, jak i funkcjonowaniu w obszarze cyberprzestrzeni - wyznaczana w drodze sądowej oceny, czy w ujęciu obiektywnym - dany obszar ludzkiej aktywności winien być oceniany, jako „prywatny". W ramach utrwalonej już linii orzeczniczej sądów stanowych oraz federalnych[94], treści w postaci danych komputerowych przetwarzanych lokalnie w domowych komputerach obywateli objęte są - na zasadzie analogii do dokumentów przechowywanych w szafie w domu - uzasadnionym oczekiwaniem prywatności, a zatem ich zatrzymanie przez organy państwowe, wymagające uprzedniego uzyskania dostępu do danych - wymaga w efekcie wydania stosownego nakazu sądowego (tzw. *search warrant*[95]). W ten sam sposób traktowane są dane wymieniane za pośrednictwem cyberprzestrzeni pomiędzy ściśle określonymi użytkownikami (np. poczta e-mail przekazywana od nadawcy do odbiorcy), jednak już nie dane, które zostały w jakiejkolwiek formie upublicznione, np. zamieszczone na stronie WWW, w otwartych zasobach sieci Internet. Zgodnie z wcześniejszą uwagą, poczta elektroniczna - jak również inne dane przekazywane za pośrednictwem sieci, tracą jednak swój „prywatny" charakter po upływie 180 dni od ich zapisania w systemach telekomunikacyjnych operatorów. Obowiązkiem uzyskania nakazu sądowego nie są natomiast obwarowane przeszukania oraz w konsekwencji zatrzymania danych przeprowadzane na podstawie zgody podmiotu uprawnionego, najczęściej - choć wcale nie zawsze, właściciela danych. Przykładowo wskazać można, iż dopuszczalność wcześniejszego wyłączenia

---

92 Ostatnio do prowadzonej dyskusji włączyły się nawet największe korporacje, jak choćby Google, stając po stronie obrony praw i wolności obywateli USA, chronionych czwartą poprawką do konstytucji. Więcej na ten temat na stronie internetowej pod adresem: http://adage.com/article/privacy-and-regulation/google-congress-update-privacy-laws-digital-age/240424/.

93 W oryginale *„reasonable expectation of privacy*". Tłumaczenie własne.

94 Za: H. M. Jarrett, M. Bailie, E. Hagen, N. Judish, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Ministerstwo Sprawiedliwości USA, s. 5 i nast. Opracowanie dostępne na stronie internetowej pod adresem: http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

95 Więcej na temat samego nakazu na stronie internetowej pod adresem: http://www.law.cornell.edu/wex/search_warrant.

poufności danych przetwarzanych przez podmioty trzecie (np. przedsiębiorcę telekomunikacyjnego) na podstawie zgody takiego podmiotu (nie zaś właściciela danych), opiera się w prawie amerykańskim nie tyle na wiążących przepisach prawa, co określanych przez te podmioty zasadach świadczenia usług. Co istotne - zgodę na przeprowadzenie przeszukania systemu oraz zatrzymanie danych w prywatnym zakładzie pracy może wydać nie tylko pracownik będący dysponentem danego systemu, ale także sam pracodawca. W zakładzie państwowym natomiast, wyłączenie obowiązku uzyskania zgody na przeszukanie zasobów systemu podlega jeszcze dalszym ograniczeniom, wyrażającym się w konieczności dokonywania każdorazowej oceny, czy dane zgromadzone w określonym systemie zakładowym - należącym przecież w tej konfiguracji faktycznej do administracji publicznej, mogą w ogóle podlegać ochronie na podstawie „uzasadnionego oczekiwania prywatności”[96].

Prezentując konstrukcję prawną czynności zatrzymania danych, przyjętą na gruncie polskiego Kodeksu postępowania karnego, należy w pierwszej kolejności zaznaczyć, iż analogicznie jak miało to miejsce w przypadku przeszukania systemu - także i tu, obowiązujące rozwiązania krajowe zostały oparte na odpowiednim stosowaniu przepisów o charakterze ogólnym. Regułę te w przypadku obydwu wskazanych czynności konstytuuje przepis art. 236a Kodeksu postępowania karnego[97] (obejmuje on swoją dyspozycją cały rozdział 25. kodeksu, zatytułowany „Zatrzymanie rzeczy. Przeszukanie”). W konsekwencji - zatrzymanie danych stanowi w pierwszej kolejności czynność realizowaną na podstawie żądania sądu lub prokuratora, zaś w przypadkach niecierpiących zwłoki - także Policji lub innego uprawnionego organu procesowego. Zgodnie z regulacją zawartą w przepisie art. 236a, rozpoczynające procedurę zatrzymania danych wezwanie do ich dobrowolnego wydania organowi prowadzącemu czynność, winno zostać skierowane do użytkownika lub dysponenta urządzenia zawierającego interesujące organ procesowy dane informatyczne lub też użytkownika lub dysponenta systemu, w którym przetwarzane są takie dane. Mając na uwadze, iż próba definicji prawnej ról procesowych określanych mianem „użytkownik” oraz „dysponent” została już przeprowadzona na gruncie rozważań dot. przeszukania zasobów systemu - rozważania te nie są powtarzane w niniejszej części rozdziału.

Z uwagi na ścisłe, wręcz genetyczne, powiązanie czynności zatrzymania danych wraz z przeszukaniem systemu (w istocie trudno wyobrazić sobie zatrzymanie zasobów cyberprzestrzeni niepowiązane z czynnością przeszukania systemu - o ile tylko zatrzymanie to

[96] Za: H. M. Jarrett, M. Bailie, E. Hagen, N. Judish, op. cit., s. 42 i nast.
[97] K. T. Boratyńska, op. cit., s. 523.

nie jest wykonywane w rozumieniu tradycyjnym wobec całego nośnika danych), należy wyrazić pogląd, iż legalny zasięg zatrzymania danych realizowanego przez polskie organy procesowe, jest zbieżny z zasięgiem dopuszczalnego na gruncie Kodeksu postępowania karnego przeszukania zasobów systemu. O ile jednak poruszana czynność przeszukania wymaga aktywnego udziału funkcjonariuszy wchodzących w różne interakcje z systemem objętym czynnością, o tyle zatrzymanie danych w istocie ogranicza się do utrwalenia danych przetwarzanych choćby ulotnie w tymże systemie (czy też innym urządzeniu), stającym się *de facto* obszarem realizacji zatrzymania danych. Innymi słowy - dane wyświetlane na ekranie komputera zlokalizowanego np. w Krakowie, podlegają faktycznej realizacji zatrzymania w obszarze pamięci właśnie tego systemu, niezależnie od faktu, czy zostały wytworzone lokalnie, czy też uprzednio pobrane z serwera znajdującego się w Niemczech, czy na terytorium USA. Powyższe stosuje się tak do pobranych plików, zapisanych historii działań *on-line,* czy wreszcie kopii maili - jak również zawartości stron WWW, choćby zagranicznych, które tylko zostały otwarte przez użytkownika systemu oraz pozostawione w pamięci komputera. Wszystkie wymienione kategorie danych lokalizują się bowiem fizycznie w jednym, krajowym systemie, występując w postaci zapisu lokalnego. Na kwalifikację tą nie ma natomiast wpływu fakt, czy określone wyżej dane zapisane są w sposób trwały, czy też wyłącznie ulotny. Prezentowaną ocenę gruntownie zmienia oczywiście ewentualna konieczność wykonania jakichkolwiek dodatkowych czynności ze strony krajowego organu procesowego, które to czynności wiązałyby się z aktywnym uzyskaniem dostępu do zasobów zlokalizowanych poza granicami kraju, np. otwarcie przeglądarki internetowej powodujące dopiero pobranie określonego materiału. Tak opisany stan faktyczny *de iure* będzie bowiem wiązał się z koniecznością uzyskania wsparcia organów zagranicznych, w ramach stosowania instytucji pomocy prawnej. Twierdzenie to stanowi konsekwencję braku międzynarodowych zasad określania zasięgu cyberjurysdykcji poszczególnych państw.

W kontekście realizacji czynności zatrzymania danych, szczególnego znaczenia prawnego nabiera także dyrektywa odpowiedniego stosowania w tym zakresie postanowień przepisu art. 217 § 5 Kodeksu postępowania karnego - stanowiącego o możliwości odebrania rzeczy w przypadku odmowy jej dobrowolnego wydania. O ile bowiem odebranie samego nośnika danych nie wydaje się nastręczać istotnych trudności interpretacyjnych, o tyle rzeczywiste, odpowiednie stosowanie wspomnianej regulacji do zatrzymania danych (w myśl dyrektywy z art. 236a) może prowadzić do wniosku, iż odmowa wydania danych, do których dostęp pozostaje np. zabezpieczony hasłem - uprawnia do podjęcia czynności odebrania

takich danych. Ponieważ przepis art. 217 § 5 nie precyzuje jednak zakresu czynności mających na celu faktyczne odebranie rzeczy - jego odpowiednie stosowanie wydaje sie być pozbawione sensu normatywnego. W szczególności, należy uznać, iż prawo do odebrania danych nie może naruszać zasady *nemo se ipsum* oraz zmierzać np. do wymuszenia na osobie odmawiającej wydania danych, udostępnienia właściwego hasła.

Zatrzymywanie danych przetwarzanych w cyberprzestrzeni może być realizowane nie tylko w odniesieniu do określonego systemu użytkownika końcowego, ale także w sieciach telekomunikacyjnych należących do operatorów oraz dostawców usług sieciowych. Regulacjami szczególnymi w tym zakresie są przepisy art. 218 oraz 218a Kodeksu postępowania karnego, nakładające na wybrane kategorie przedsiębiorców świadczących usługi z zakresu telekomunikacji, obowiązki zatrzymywania oraz wydawania danych transmitowanych poprzez sieci na rzecz podmiotów uprawnionych[98]. Wydanie takie - obejmujące w istocie wszelkie dane, które tylko zostały przekazane za pośrednictwem cyberprzestrzeni, następuje na podstawie postanowienia sądu lub prokuratora. Postanowienie takie może także zmierzać nie tyle do wydania, co samego zabezpieczenia danych (art. 218). Zabezpieczenie takie może jednak zostać zarządzone wyłącznie na czas oznaczony, nieprzekraczający 90 dni. Należy uznać, iż podstawowym celem zabezpieczenia danych jest ich czasowe utrwalania celem późniejszego przeprowadzenia czynności właściwego zatrzymania danych.

Mając na uwadze powyższe rozważania, należy ostatecznie stwierdzić, iż - analogicznie, jak w przypadku realizacji czynności przeszukania zdalnego, także zdalne zatrzymanie (to jest wykonywane za pośrednictwem sieci, bez udziału osób trzecich względem przedstawicieli organu procesowego) nie znajduje jakichkolwiek podstaw prawnych na gruncie obowiązujących przepisów Kodeksu postępowania karnego. Z uwagi na niemożliwość zachowania przewidzianych prawem rygorów procesowych w przypadku wykonywania zdalnego zatrzymania danych, czynność ta nie może stanowić źródła materiału dowodowego w rozumieniu procesowym. Ewentualne dane - zatrzymane faktycznie np. w drodze zapisania przez funkcjonariusza kopii strony WWW zawierającej treści nielegalne, nie mogą zatem stanowić bezpośrednio dowodu w postępowaniu karnym, wymuszając ich procesową walidację w drodze przeprowadzenie innych, procesowych już czynności dowodowych. Czynnością taką w szczególności może być przesłuchanie w charakterze świadka funkcjonariusza, który wykonał ową kopię strony, co powoduje

98 *Ibidem*, s. 506.

iż utrwalone wcześniej pliki stają się wówczas swoistym materiałem uzupełniającym. Poprawna interpretacja wprowadzanego w ten sposób materiału - z uwagi na wysoce techniczny charakter, może wymagać zastosowania wiedzy o charakterze specjalnym, co wiązać się będzie w tej sytuacji z koniecznością powołania w procesie biegłego z zakresu teleinformatyki, czy też informatyki śledczej.

PODSUMOWANIE

Podsumowując najważniejsze tezy niniejszego rozdziału należy wskazać na następujące zagadnienia prawne:

– specyfika obszaru cyberprzestrzeni, definiowanego w sposób niematerialny, pozbawiony fizycznej wymierności, w sposób istotny odciska się nie tylko na sposobie pojmowania nowoczesnych form przestępczości, ale także na rozumieniu czym stają się czynności procesowe, które podejmowane są w poruszanym obszarze domeny cyfrowej,
– choć cele procesu karnego pozostają niezmienne w stosunku do każdego rodzaju przestępczości, środki prawne stosowane dla wykrywania, utrwalania odnośnych dowodów oraz ustalania i osądzania sprawców przestępstw popełnianych w cyberprzestrzeni muszą dostosowywać się do nowych wymagań oraz możliwości, które pojawiły się wraz z szeroką popularyzacją rozwiązań teleinformatycznych, pośród których szczególne miejsce zajmuje rozwój globalnej sieci Internet,
– do obszarów wymagających szczególnego dostosowania sposobu pojmowania czynności procesowych w odniesieniu do cyberprzestrzeni należą kwestie związane z określeniem przedmiotu czynności procesowej realizowanej w obszarze cyberprzestrzeni, kwestie umiejscowienia tak określonej czynności (w cyberprzestrzeni - czyli gdzie?), szczególna charakterystyka materiału dowodowego występującego w postaci danych, możliwość jego bezstratnego (wręcz idealnego) powielania - stanowiącego w ujęciu technicznym w istocie jedyny sposób utrwalenia materiału dowodowego, czy wreszcie problematyka wyznaczania zasięgu tzw. cyberjurysdykcji poszczególnych państw w domenie cyfrowej. Zagadnienia te, z uwagi na swoją złożoność, mogą zostać w niniejszym podsumowaniu jedynie przywołane hasłowo,

- problematyka cyfrowej morfologii obszaru cyberprzestrzeni pozostaje nierozerwalnie związana z poprawnym rozumieniem, czym są dane informatyczne - rodzajowo budujące zarówno materiał dowodowy, przedmiot wykonawczy, jak i najczęstszy cel ataku przestępstwa popełnionego w cyberprzestrzeni. Postulat ten pozostaje nie do przecenienia w kontekście określania specyfiki transpozycji czynności procesowych do obszaru domeny cyfrowej,
- istotnym zagadnieniem prawnym związanym z realizacją czynności procesowych w cyberprzestrzeni pozostaje także problematyka wyznaczenia zakresu dopuszczalnej ingerencji w prawa i wolności człowieka i obywatela - który podłączając się do zasobów globalnej sieci Internet, pozostaje narażony w znacznie wyższym stopniu na nieuprawnione ingerencje ze strony zarówno przestępców, jak i organów administracji państwowej, niż ma to miejsce przy prowadzeniu działalności konwencjonalnej, umiejscawiającej się w przestrzeni fizycznej. Kwestia ta zarysowuje się szczególnie wyraźnie na tle realizacji tzw. przeszukań zdalnych oraz zdalnych zatrzymań, będących czynnościami wykonywanymi *on-line*, to jest za pośrednictwem sieci, bez udziału osób, których czynności te dotykają, a co więcej - najczęściej w sposób niejawny, pozostający w ukryciu przed użytkownikami systemów objętych działaniem organów państwowych,
- z punktu widzenia procesowego, konieczne jest wreszcie aby organizując wyobrażenie procesu karnego prowadzonego w sprawie o cyberprzestępstwo nie tracić z pola widzenia niezbędnej korelacji czynności dowodowych podejmowanych wewnątrz obszaru cyberprzestrzeni, z czynnościami realizowanymi poza jej zakresem. Powoływanie funkcjonariuszy pionów technicznych organów procesowych w charakterze czy to świadków, czy też biegłych, stanowi bowiem istotne uzupełnienie postępowania w sprawie o czyn, który choć skonsumowany w obszarze rzeczywistości wirtualnej, podlega ocenie dokonywanej przez ludzi, funkcjonujących zawsze wyłącznie w świecie rzeczywistym,
- procesowe ujęcie czynności realizowanych w ramach postępowania karnego w sprawie o przestępstwo popełnione w cyberprzestrzeni wymaga ustawicznego stosowania wiedzy zarówno prawniczej, jak i przynajmniej podstawowej wiedzy z zakresu szeroko rozumianej teleinformatyki. Z uwagi na postępującą specjalizację, faktyczna realizacja czynności procesowych podejmowanych we wskazanym obszarze

nabiera coraz silniejszych konotacji technicznych, stając się powodem dla powoływania specjalnych jednostek właściwych w zakresie tzw. informatyki śledczej,

- ostatecznie, mając na uwadze powyższe tezy, specyfika cyberprzestrzeni warunkuje konieczność zupełnie nowego spojrzenia prawnego na podstawowe czynności procesowe, jak analizowane w niniejszej pracy przeszukanie zasobów systemu teleinformatycznego oraz zatrzymanie danych. Czynności te - po ich transpozycji do świata cyberprzestrzeni, nabierają bowiem zupełnie nowego wydźwięku, skłaniając do interpretowania na nowo wielu przepisów, które pierwotnie powstawały z myślą o realizacji zadań procesowych w otaczającym nas świecie fizycznym, dającym się opisać za pomocą wymiarów oraz znanych właściwości fizycznych,
- całokształt powyższych zagadnień skłania ostatecznie do wysunięcia dodatkowego wniosku o konieczności ujmowania zagadnień związanych z obszarem cyberprzestrzeni w nowych ramach prawnych, które pozwalałyby na bezpośrednie uwzględnianie specyfiki obszaru cyfrowego, bez konieczności odwoływania się w tym zakresie do nierzadko utrudnionych, a praktycznie zawsze niejednoznacznych, interpretacji prawnych wynikających z odpowiedniego stosowania regulacji konwencjonalnych wobec opisu prawnego niemacalnej rzeczywistości cyberprzestrzeni.

Wnioski

Przeprowadzone na gruncie rozdziałów niniejszej pracy rozważania prawne pozwalają na sformułowanie szeregu wniosków, odnoszących się tak do charakterystyki cyberprzestrzeni, opisu zjawiska cyberprzestępczości, jak i zasad transpozycji czynności procesowych do świata domeny cyfrowej. Wnioski te służą następnie do wyprowadzenia szeregu postulatów odnoszących się nie tylko do zagadnień interpretacji przepisów obowiązujących, ale także kierunków przyszłych zmian w prawie.

Tezą niniejszej pracy było założenie prawne, iż specyfika techniczna (faktyczna) cyberprzestrzeni zmodyfikowała sposób pojmowania typowych instytucji prawnych w stopniu tak istotnym, iż wymagają one nowego podejścia interpretacyjnego lub wręcz zasadniczego przeformułowania ich konstrukcji prawnych. Twierdzenie to dotyczy w szczególności szeroko omawianych w pracy, nowoczesnych form przestępczości komputerowej, której liczne przejawy nie mogłyby w ogóle zaistnieć, gdyby nie faktyczne pojawienie się zupełnie nowej domeny cyberprzestrzeni. Jej fizycznie nienamacalna, cyfrowa rzeczywistość, która charakteryzowana jest przez żelazną logikę komputerów oraz sieciową *bezterytorialność* odkryły zupełnie nowe dobra prawne wyznaczane w szczególności zakresem ochrony prawnej niezakłóconej pracy systemów teleinformatycznych oraz ich zasobów, stanowiących dziś wartość niejednokrotnie najistotniejszą dla nowoczesnych przedsiębiorstw, ale także państw. Coraz częściej bowiem, od poprawnego działania komputerów zależy wręcz ludzkie życie, które może zostać zagrożone choćby drobną dysfunkcją systemów monitorujących np. pracę elektrowni. Postępująca informatyzacja sprawiła, iż komputery oraz budowane przez nie sieci stały się aktualnie nieodzowną częścią współczesnej geografii świata.

Zarysowana w powyższy sposób teza została w niniejszej pracy nie tylko potwierdzona szczegółowymi rozważaniami na temat budowy cyberprzestrzeni oraz analizą fenomenu cyberprzestępczości, ale także rozwinięta w licznych obszarach szczegółowych odnoszących się do zagadnień *budowy* zasobów komputerowych stanowiących dowody elektroniczne, możliwości ich swobodnego powielania, budowy tzw. dokumentów elektronicznych - w tym kwestii ich podpisu, zagadnień zabezpieczania danych poprzez ich szyfrowanie, czy wreszcie kwestii faktycznego podejmowania określonych działań w cyberprzestrzeni, jak choćby realizacji przeszukania systemu, wykonywanego czy to

z zachowaniem bezpośredniego kontaktu z systemem, czy też za pośrednictwem sieci, to jest *on-line*.

Formułowane w niniejszej części pracy wnioski oraz postulaty zostały podzielone na trzy części, odnoszące się kolejno - analogicznie, tak jak tok samego wywodu, do ujęcia prawnego definicji cyberprzestrzeni, kwestii związanych z regulacją zjawiska cyberprzestępczości oraz ostatecznie przeniesienia realizacji czynności procesowych do obszaru domeny cyfrowej.

Wnioski oraz postulaty w zakresie definicji prawnej cyberprzestrzeni.

Zebrane w rozdziałach 1 – 3 niniejszej pracy rozważania oraz uwagi dotyczące narodzin i dalszego kształtowania się cyberprzestrzeni, pozwalają stwierdzić iż mamy w tym przypadku do czynienia z jednoznacznym ukształtowaniem się nowej domeny ludzkiej aktywności, posiadającej nieznaną wcześniej cechę „wirtualności" zaś pozbawioną znanych cech fizycznych, jak wymiary, odległości, czy topografia geograficzna. Istotą cyberprzestrzeni nie jest bowiem podbudowujący ją sprzęt komputerowy, czy też prosta możliwość zestawiania połączeń pomiędzy dowolnymi zakończeniami (to oferuje bowiem już telefonia) zaś globalna przestrzeń współżycia ludzi wchodzących ze sobą w nieskrępowane interakcje, w tym interakcje prawne - cywilne, administracyjne, ale również karne. Jako główne cechy tak postrzeganej domeny cyfrowej wskazać należy w szczególności, iż:

- cyberprzestrzeń to zupełnie nowy jakościowo, cyfrowy oraz globalny obszar o charakterze logicznym, w którym nie obowiązują zasady fizyki, czy też znana ze świata fizycznego wymiarowość. Cyberprzestrzeni nie należy kojarzyć z budującą ją infrastrukturą sieciową - choć nie wątpliwie bez tej infrastruktury cyberprzestrzeń nie mogłaby istnieć. Istotą omawianej domeny nie jest jednak jej warstwa fizyczna (ta bowiem pozostaje transparentna dla użytkowników stanowiąc jedynie podbudowę omawianego obszaru), lecz szeroko rozumiana warstwa usługowa, czy też warstwa działania użytkowników, na poziomie której przetwarzane są dane. Dane te mogą stanowić stanowią bądź to odzwierciedlenie znanych już dóbr prawnych, bądź też stanowić ucieleśnienie zupełnie nowych wartości, które w ogóle nie mogłyby zaistnieć bez faktycznego wykształcenia się obszaru cyberprzestrzeni. Do pierwszej z tak wyróżnionych kategorii zaliczyć można przede wszystkim:

- przedmioty własności intelektualnej,
- dane budujące wszelkiego rodzaju komunikaty, jak wiadomości poczty elektronicznej, przekazy wymieniane za pomocą komunikatorów, materiały audio-wizualne (zdjęcia filmy), będące przedmiotem ochrony przede wszystkim tajemnicy komunikacyjnej,
- płatnicze lub usługowe środki przedpłacone (wszelkie formy kart *prepaid*),
- usługi np. sklepowe, czy e-bankowości pozwalające zarządzać aktywami.

Jako przykłady przedmiotów ochrony prawnej, które mogły faktycznie zaistnieć dopiero po wytworzeniu obszaru cyberprzestrzeni wskazać natomiast można np.:

- istniejące wyłącznie w formie zapisu danych usługi sieciowe, jak choćby wirtualne dyski, rozwiązania chmurowe, czy też prawa dostępu do serwisów WWW, portali lub kont, czy wreszcie rozwiązania bazodanowe,
- szczególne rozwiązania sieciowe stanowiące odrębny przedmiot ochrony intelektualnej, np. specyficzne ustawienia konfiguracyjne, indywidualne metody weryfikacji i uwierzytelniania użytkowników, czy też sama architektura określonych technologii programowych,
- usługi bezpieczeństwa, polegające na ochronie systemów teleinformatycznych oraz sieci, realizowane zarówno pasywnie (wszelkie formy monitorowania pracy sieci oraz generowanego w niej ruchu) oraz aktywnie (systemy antywirusowe, tzw. heurystyka ruchu sieciowego itd.),
- oraz te najbardziej osobliwe – własność istniejących wyłącznie wirtualnie „przedmiotów" wykorzystywanych w różnego rodzaju portalach sieciowych, czy grach komputerowych,

- cyberprzestrzeń jest obszarem sztucznym, zaprojektowanym w pełni przez człowieka lecz doświadczalnym wyłącznie z zastosowaniem urządzeń teleinformatycznych. Z uwagi na cyfrową budowę, poruszanie się po cyberprzestrzeni rządzone jest w efekcie innymi zasadami niż poruszanie się po *fizycznej* rzeczywistości. W szczególności, cyberprzestrzeń, będąca obszarem pozbawionym typowo

przestrzennej konotacji wymyka się prostemu poznaniu „miejsca” w którym się przebywa lub „odległości” dzielącej poszczególne obiekty. Różnice te powodują m.in. konieczność zupełnie nowego pojmowania granic dzielących własność poszczególnych użytkowników sieci, ale również granic państwowych. Zasady poprawnego poruszania się po sieci oraz swoiste zasady sieciowego współżycia społecznego wynikają najczęściej ze swoistych, niepisanych konwenansów sieciowych. Wiele z nich nie znajduje jednak żadnych podstaw prawnych, wymykając się kwalifikacji prawnej, jak choćby wykorzystywanie ogólnie dostępnych funkcji sieciowych, które w określonych warunkach mogą nawet zmienić swojej zastosowanie z typowo systemowego, np. diagnostycznego, na ofensywne, czy wręcz przestępne, mogące zakłócić poprawną pracę systemu teleinformatycznego obranego za cel takiego działania,

- cyberprzestrzeń, stanowiąc obszar nieskrępowanej fizycznymi atrybutami działalności człowieka, wykształciła szereg nowych interakcji międzyludzkich. Ich przykładami mogą być chociażby fenomen portali społecznościowych, działanie rozlicznych for internetowych, czy możliwość prowadzenia własnych witryn *bloggerskich*, stających się nowymi zjawiskami kulturowymi o potencjalnie ogromnej sile oddziaływania społecznego. Dodając do tego atrybut globalności sieci – cyberprzestrzeń stanowi obszar wolnej wymiany poglądów, idei oraz myśli, będąc nie tylko zjawiskiem *komercyjnym* ale także społecznym, poddającym się wszelkim badaniom socjologicznym,

- jedynym budulcem zasobów cyberprzestrzeni są bity danych, charakteryzujące się w szczególności możliwością bezstratnego powielania, bezstratnego wykorzystania (dane nie podlegają degradacji) oraz przesyłania na nieograniczone odległości. Co istotne, dane poddają się także szeregu dalszych bezstratnych przekształceń, jak choćby związanych z ich szyfrowaniem celem uniemożliwienia odbioru przez osoby postronne (w tym jednak także podmioty uprawnione do prowadzenia czynności operacyjnych, czy procesowych). Każda informacja zawarta w cyberprzestrzeni, w tym każdy przekaz, wiadomość email, dowolny obraz lub nagranie dźwięku, ale także pracujące na komputerach aplikacje, muszą być zatem postrzegane na poziomie pracy systemów jako ciągi binarne, składające się z kombinacji zer i jedynek. To właśnie one stanowią jedyny „realny” wymiar przedmiotów poddawanych ochronie prawnej w cyberprzestrzeni,

- z uwagi na swoje cechy, cyberprzestrzeń – stanowiąca wyłącznie obszar logiczny, odrywa się od możliwości przypisywania jej cech geograficznych, w tym jakichkolwiek wymiarów, jak długość, czy szerokość, wymykając się znanym powszechnie zasadom jurysdykcji. O ile bowiem możliwe jest dokonanie ustalenia, na terytorium którego z państw znajduje się określone fizyczne zakończenie sieciowe wykorzystywane do obsługi ruchu w ramach określonej transmisji danych, o tyle już jednoznaczne wskazanie „miejsca" pracy systemu realizującego określoną usługę sieciową, która wykonywana jest w pełnej współpracy z szeregiem systemów (nierzadko rozsianych po całym świecie) nie poddaje się takiej kwalifikacji (np. zwykłe otwarcie strony internetowej powoduje nie tylko pracę komputera, na którym dokonuje się tego otwarcia, ale także serwera WWW na którym znajduje się dana strona, uprzednio serwera DNS ustalającego dokładny adres IP strony oraz wszystkich serwerów pośredniczących w transmisji ruchu od nadawcy do odbiorcy w ramach tzw. trasowania). Cyberprzestrzeń pozostaje także tworem globalnym, którego nawet najodleglejsze węzły łączone są obecnie w części sekundy. Wszelkie zasoby podłączone do cyberprzestrzeni stają się w konsekwencji natychmiastowo zasobami globalnymi, technicznie możliwymi do osiągnięcia przez dowolnego użytkownika cyberprzestrzeni, już bez zapewniania żadnych dodatkowych rozwiązań technicznych lub organizacyjnych, niczym pozostawienie przedmiotu własności prywatnej w publicznie dostępnej przestrzeni, otwartej na widok każdego przechodnia,

- cyberprzestrzeń zawiera zasoby zarówno prywatne, jak i państwowe, stając się domeną zróżnicowanych działań: osobistych, komercyjnych, administracyjnych, ale także przestępnych, wywiadowczych, czy terrorystycznych. W ślad za rozwojem rynku usług oferowanych w cyberprzestrzeni, coraz większa część naszego codziennego życia przenosi się do domeny cyfrowej, stającej się w konsekwencji istotną wartością ale także potencjalnym źródłem nielegalnego zysku, a nawet celem działań typowo ofensywnych, w tym militarnych,

- cyberprzestrzeń pozostaje przestrzenią otwartą, rozszerzalną oraz w pełni skalowaną. Nie mając granic, cyberprzestrzeń nie posiada także żadnych ograniczeń w zakresie dalszego rozwoju, tak ilościowego (ustawiczne powiększanie przestrzeni dyskowej macierzy, wzrost liczby oraz wielkości przetwarzanych zasobów, wzrost przepustowości łączy transmisyjnych), jak i jakościowego (nowe rodzaje usług, które zaledwie kilka lat temu pozostawały wyłącznie w fazie koncepcyjnej).

Powyższy opis cech technicznych cyberprzestrzeni implikuje szereg wniosków *stricte* prawnych, odnoszących się do sposobu legalnego postrzegania omawianej domeny cyfrowej:

- poprawne zdefiniowanie (oraz zrozumienie) prawne istoty cyberprzestrzeni wymaga otwarcia na szerokie spektrum cech specyficznych nowej domeny. Cechy te - posiadające swoje określenia techniczne, są uwzględniane w obowiązujących przepisach nie tylko częściowo, ale także w sposób rozpropagowany w różnych aktach prawnych, w zależności od rodzaju materii regulowanej w danym dokumencie. To, czym cyberprzestrzeń jest w ujęciu prawnym musi być w konsekwencji rekonstruowane na podstawie analizy prawnej licznych aktów normatywnych oraz aktów o charakterze politycznym odnoszących się tak do gałęzi prawa karnego, cywilnego, jak i administracyjnego. Jako wniosek należy w tym zakresie podnieść zasadność uporządkowania odnośnych przepisów pod kątem stosowanej w nich siatki pojęciowej, tak by każda z ustaw branżowych posługiwała się jednolitym, wspólnym aparatem pojęciowym – a w konsekwencji także interpretacyjnym,
- obszar cyberprzestrzeni wymyka się definiowanemu tradycyjnie władztwu państwowemu. Działania państw w cyberprzestrzeni wymagają określenia nowych zasad tzw. cyberjurysdykcji, która w szczególności odrywa się od geograficznych granic terytorialnych. W ocenie autora - wypracowane zasady muszą być równie globalne, co sama cyberprzestrzeń. Globalizacja cyberjurysdykcji wymaga natomiast ustalenia reguł kolizyjnych ustalania właściwości państw w przypadku, gdy kwalifikowane prawnie działanie dotyka obywateli podlegających jurysdykcji różnych - często wielu, systemów prawnych (np. obywatel Niemiec przeprowadza cyberatak przeciwko obywatelowi Angielskiemu, którego wykradane dane przechowywane są na serwerach ulokowanych na terytorium USA). W sytuacjach takich działania procesowe winny być podejmowane w pełnej współpracy organów ścigania wszystkich zaangażowanych państw, co dla utrzymania efektywności wymaga jednak przyjęcia jednolitych zasad prawnych w zakresie reagowania na występujące incydenty oraz ataki cybernetyczne. Współpraca poszczególnych państw nie może zostać wyłączona na rzecz przejęcia właściwości prawnej przez jedno z nich (np. państwo obywatela pokrzywdzonego) z uwagi brak uprawnień do wykonywania

czynności faktycznych, jak choćby zatrzymanie osoby, czy rzeczy lub prowadzenie ustaleń (np. odpytywanie operatorów telekomunikacyjnych o dane dot. ruchu sieciowego) przez organy procesowe jednego państwa na terytorium państwa obcego,

- niezbędnym elementem budowy globalnych zasad jurysdykcji cybernetycznej jest przyjęcie wspólnego katalogu cyberprzestępstw oraz określenie jednolitego systemu kar, zapewniające wypełnianie zasady podwójnej karalności przez sprawcę działającego transgranicznie. W szczególności należy podkreślić konieczność harmonizacji prawa w zakresie stosowanych przesłanek uznania danego działania za czyn bezprawny, gdzie pierwszorzędnej wagi nabiera ustalenie, czy atak był skierowany na dane, budowane z nich informacje, czy też szeroko rozumianą warstwę usługową, która jest realizowana (oraz analogicznie może być atakowana) w sposób w pełni zautomatyzowany (uwaga rozszerzona w kolejnej części wniosków, poświęconej kwestiom samego ujmowania cyberprzestępstw),

- istotnym elementem ujęcia prawnego cyberprzestrzeni winno być także uwzględnianie jej specyficznych zasobów oraz pojawiających się na tym tle uprawnień oraz kompetencji organów ścigania, odpowiedzialnych za bezpieczeństwo w cyberprzestrzeni. Niezbędne jest w szczególności zdefiniowanie pojęcia „dowodu elektronicznego", którego zasady przetwarzania różnią się w sposób istotny od zasad przetwarzania dowodów fizycznych (m. in. możliwością bezstratnego powielania, w tym bezstratnego pozyskiwania za pośrednictwem sieci). W szczególności, definicja legalna dowodu elektronicznego winna odrywać się od jego substratów fizycznych, jak nośnik danych, na których określony zasób został zapisany. Niezbędne jest przy tym ujęcie prawne zasad oceny autentyczności tej postaci dowodów, które z racji na swoją specyfikę, mogą podlegać niezauważalnym dla laika, nieuprawnionym modyfikacjom. Uwaga ta, co warto zaznaczyć, znajduje swoje zastosowanie tak w odniesieniu do rozważań prowadzonych na gruncie prawa karnego, jak i pozostałych gałęzi prawa, w tym prawa cywilnego oraz administracyjnego,

- zasady dopuszczalnego prawnie korzystania z zasobów cyberprzestrzeni winny zostać wyznaczone poprzez precyzyjnie sformułowane katalogi *elektronicznych* dóbr prawnie chronionych (np. samo bezpieczeństwo systemu) oraz cyberprzestępstw, nie pozostawiające wątpliwości, co do kwalifikacji prawno-karnej działań użytkowników

systemów teleinformatycznych. Działania nie ujęte, jako karalne, winny pozostawać jednoznacznie legalne,

- ostatecznie, niezbędne jest także określenie wymogów prawnych w zakresie stosowania w cyberprzestrzeni zabezpieczeń kryptograficznych, mogących uniemożliwiać organom państwowym realizację ich ustawowych zadań,
- mając na uwadze powyższe wnioski, należy wyrazić aprobatę dla faktu przyjęcia do polskiej ustawy definicji pojęcia „cyberprzestrzeń", która to definicja winna jednak być traktowana wyłącznie jako punkt wyjścia dla dalszych prac legislacyjnych mających na celu uwzględnienie w systemie prawa sygnalizowanych zagadnień.

Wnioski oraz postulaty w zakresie regulacji zjawiska cyberprzestępczości.

Konsekwencją opisanych wyżej cech szczególnych cyberprzestrzeni stała się konieczność wypracowania nowych metod badawczych w stosunku do przestępczości cybernetycznej. Cechy globalności oraz wirtualności zasobów cyberprzestrzeni stały się bowiem przyczynkiem do wytworzenia nieznanych uprzednio form oraz metod działań bezprawnych, wykorzystujących w szczególności innowacyjność nowego obszaru oraz bardzo często brak jego jasnych ram organizacyjno-prawnych. Poczynione na gruncie rozdziałów 2 i 4 niniejszej pracy rozważania pozwalają sformułować następujące uwagi odnoszące się do sposobu regulacji prawnej poruszanej gałęzi działalności przestępnej:

- jako podstawową uwagę normatywną należy wskazać na zasadność jasnego zdefiniowania charakteru prawnego przestępczości komputerowej, która w niniejszej pracy określana była w szczególności, jako przestępczość popełniana w stosunku do przedmiotów ochrony ucieleśnianych w zasobach cyberprzestrzeni (opisowo - przestępczość cybernetyczna *sensu stricte*) oraz przestępczość związana z dystrybucją określonych, nielegalnych treści (ujęta w rozumieniu pojęcia przestępczości cybernetycznej *sensu largo*). W tak wyszczególnionych przypadkach systemy komputerowe występują bądź to jednocześnie w roli narzędzi oraz celu ataku , bądź też wyłącznie jako narzędzie do popełnienia przestępstwa, które nierzadko może zostać dokonane także przy wykorzystaniu innego medium informacji lub wręcz ustanie (np. znieważenie lub propagacja określonych treści w formie ulotek),

- aktualnie funkcjonującą w krajowych porządkach prawnych oraz zarysowywaną w systemie prawa międzynarodowego typizację przestępstw cybernetycznych należy uznawać za niepełną. Twierdzenie to wynika w ocenie autora pracy z ciągłego przenoszenia na grunt cyberprzestrzeni sposobu pojmowania działań bezprawnych właściwego dla przestępczości konwencjonalnej. Brak pełnego ujęcia specyfiki cyberprzestrzeni oraz realnych możliwości przestępczości cybernetycznej skutkuje w efekcie definiowaniem tej gałęzi działalności bezprawnej tworzeniem regulacji typowo *materialnych*, kierujących się wobec fizycznie wyodrębnionego przedmiotu ataku. Poza zakresem regulacji karnych pozostaje szereg powszechnie identyfikowanych czynności technicznych o jednoznacznie bezprawnym zabarwieniu, jak w szczególności:

    - tworzenie szczególnych warunków dla podszywania się w sieci pod inne osoby lub też tworzenie warunków do popełnienia przestępstwa cybernetycznego poprzez infrastrukturę osoby trzeciej - czyn ten nie stanowiąc formy faktycznego dokonania podszycia się pod wybraną osobę fizyczną (lub podmiot o charakterze prawnym) nie zawsze przybiera postać oszustwa komputerowego, mogąc polegać np. na przeprowadzaniu dowolnego cyberataku z wykorzystaniem niezabezpieczonej sieci bezprzewodowej należącej do osoby fizycznej. Działanie takie ma na celu przede wszystkim skierowanie podejrzeń o sprawstwo danego ataku na właściciela nieświadomie udostępnionego łącza sieciowego oraz ukrycie prawdziwego sprawcy działań,

    - tworzenie szczególnych warunków do popełnienia przestępstwa komputerowego, jak skanowanie portów, czy poszukiwanie luk bezpieczeństwa, mające na celu ustalenie słabych stron danego systemu celem jego infiltracji, zakłócenia lub nawet wymuszenia haraczu za odstąpienie od ataku (ta ostatnia forma zjawiskowa najczęściej przybiera postać swoistej propozycji „usługi” bezpieczeństwa, polegającej na odpłatnym wskazaniu wykrytych w systemie podatności bezpieczeństwa),

    - tworzenie zdalnie sterowanych sieci tzw. komputerów zombie (nazywanych sieciami *botnet*), służących do przeprowadzania wybranych - w istocie najgroźniejszych oraz najrozleglejszych w skali, rodzajów ataków cybernetycznych. O ile pozyskiwanie poszczególnych komputerów i ich

włączanie do tego typu sieci najczęściej wiąże się z przełamaniem ich zabezpieczeń, co już konstytuuje czyn karalny, o tyle organizowanie sieci *botnet* z uwagi na swoją specyfikę oraz w szczególności zamiar sprawcy, obejmujący w tym przypadku utworzenie cybernetycznej broni masowego rażenia – winno znajdować swoją szczególną penalizację karną o znacznie podniesionej sankcji, czy wreszcie,

    - legalne wykorzystywanie funkcji, dostępnych nawet w samych systemach operacyjnych, do wywoływania wszelkiego rodzaju niepożądanych przez użytkownika efektów, jak choćby uporczywe odpytywanie jego systemu o czas reakcji (tzw. *ping*).

- istotną cechą przestępczości cybernetycznej jest fakt, iż jej przejawy poznawalne są wyłącznie z zastosowaniem szeroko rozumianych narzędzi teleinformatycznych. W tym kontekście, zwalczanie oraz wykrywanie cyberprzestępczości może być prowadzone jedynie z zastosowaniem specjalistycznych technik oraz narzędzi, których stosowanie narzuca wysoko techniczny charakter faktycznego opis tej gałęzi przestępczości. Poprawne ujmowanie przesłanek prawnych stosowanych dla opisu poszczególnych przestępstw cyberprzestrzeni winno zatem uwzględniać owe kwestie techniczne, tak by nie prowadzić do daleko idących rozbieżności w sposobie definiowania przestępstwa na poziomie prawnym oraz merytorycznym. Pozostawiając oczywistym, iż język prawa nie może zostać zastąpiony żargonem technicznym stosowanym przez tzw. cybeśledczych, jako uwagę ogólną należy jednak w ocenie autora pracy podnieść zasadność postępującego uwzględniania w obowiązujących przepisach opisów przestępstw uwzględniających ich szczególny, techniczny charakter,

- pozostając w kręgu uwag definicyjnych – zasadne jest także ujednolicenie stosowanej na gruncie przepisów krajowych siatki pojęciowej odnoszącej się do taksonomii systemów (teleinformatycznych/informatycznych), urządzeń oraz nośników,

- wszelkie faktyczne przejawy przestępczości komputerowej powinny być odnoszone do danych, nie zaś informacji, jako zarówno przedmiotu przestępstwa, jak i narzędzia jego popełnienia. Stosowane w polskim porządku prawnym typizowanie cyberprzestępstw, jako czynów skierowanych przeciwko informacjom nie pozwala na

jednoznaczne ustalenie karalności czynów polegających na wykradzeniu np. jedynie części pliku (określonej porcji danych) nie składającej się jednak na pełną informację, czy też danych danych budujących informację występującą w postaci zaszyfrowanej (do czasu dekryptażu takiej informacji, sprawca czynu nie może zostać *de iure* oskarżony o bezprawne zapoznanie się z treścią zasobu). Jednoznaczne oraz konsekwentne odnoszenie się w sposobie typizacji przestępstw do danych posiada zatem swoje ścisłe uzasadnienie merytoryczne (odnoszące się do opisanej w pracy budowy cyberprzestrzeni), ale niesie za sobą niezwykle istotne implikacje prawne. Implikacje te należy pojmować także w dodatkowym kontekście funkcjonowania cyberprzestępczości, która może być popełniana także w sposób zautomatyzowany, z wykorzystaniem uprzednio przygotowanego oprogramowania, które po wpuszczeniu do sieci samoistnie próbuje pozyskać określone aktywa, jak hasła, loginy, czy kody prepaid. W tym przypadku nie można byłoby uznawać, iż działający samodzielnie już program w ogóle „zapoznaje się" z jakimikolwiek informacjami,

- jako osobne dobro prawnie chronione w systemie prawa karnego winno występować także samo niezakłócone lub niezmienione funkcjonowanie systemów teleinformatycznych. Czyny kierowane przeciwko tak nazwanym wartościom prawnym nie muszą dążyć do naruszenia jakichkolwiek atrybutów bezpieczeństwa danych, wpływając wyłącznie na sposób działania określonego systemu niezgodnie z wolą jego dysponenta prawnego. Czyn taki nie musi dążyć do obniżenia wydajności systemu, zaś może wyłącznie ograniczać się do nieuprawnionego ingerowania w działanie urządzenia, jak np. zdalne instalowanie oprogramowania służącego do przekazywania treści reklamowych, czy oprogramowania gromadzącego wybrane kategorie danych o ruchu sieciowym użytkownika celem rzekomego podwyższania jego bezpieczeństwa w sieci - co stanowi aktualnie częsty element działania tzw. programów antywirusowych. Działania takie mogą godzić w szczególności w prawo do prywatności użytkownika (np. śledząc jego poczynania w sieci dla celów marketingowych lub statystycznych), zapewniać narzędzie transmisji niezamawianych treści (w tym dodatkowo płatnych w ramach udziału w określonej usłudze) bądź też nawet stanowić formę nękania. Wyłączenie karalności tego typu działań w cudzym systemie winno wymagać jednoznacznej oraz w pełni świadomej zgody użytkownika systemu,

- karalność cyberprzestępstw winna uwzględniać fakt, iż ataki cybernetyczne mogą być wykonywane zarówno poprzez bezpośrednie działanie sprawcy ataku, jak również działanie zaprogramowane oraz zadane np. przygotowanemu wirusowi komputerowemu. Wirus taki (lub szerzej, dowolny inny rodzaj oprogramowania złośliwego) może działać w pewnym sensie suwerennie, rozprzestrzeniając się po cyberprzestrzeni w sposób nie poddający się już żadnej kontroli jego autora, czy osoby oryginalnie propagującej takie oprogramowanie w cyberprzestrzeni. Czyny takie powinny podlegać odrębnej karalności, jako nastawione nie tyle przeciwko konkretnemu systemowi lub ich grupie, co powodujące zagrożenie dla bezpieczeństwa cybernetycznego wszystkich użytkowników sieci. Jako szczególną kategorię tego typu przestępczości należy wyróżnić opracowywanie narzędzi dedykowanych do przeprowadzania ataków typu APT, nakierowanych w sposób specyficzny na określony krąg podmiotów (np. firmy określonej branży – atak przybiera wówczas najczęściej postać szpiegostwa gospodarczego lub może nosić cechy quasi terrorystyczne – gdy kieruje się np. przeciwko określonemu rodzajowi instalacji usługowych, w tym elementów infrastruktury krytycznej kraju),
- niezbędne jest prawne zdefiniowanie pojęć odnoszących się do naruszania lub też omijania zabezpieczeń systemów teleinformatycznych, stanowiących aktualnie elementy typizacji określonych kategorii cyberprzestępstw. Należy mieć na uwadze, iż specyficzna charakterystyka obszaru cyberprzestrzeni nie pozwala kwalifikować tak ujmowanych zachowań sprawcy z odwoływaniem się do zasad codziennego życia, sprawdzających się w otaczającym nas świecie fizycznym. W pewnym uproszczeniu, można powiedzieć, że analogią do ominięcia prymitywnego lub też zwyczajnie słabego zabezpieczenia teleinformatycznego może być wejście na teren nieoznakowanej oraz nieogrodzonej posesji, na której jednej z krawędzi stoi zupełnie oderwana od otoczenia brama. Niezbędne jest w tym kontekście zdefiniowanie prawne - wzorem regulacji międzynarodowych, treści pojęcia czynu bezprawnego w cyberprzestrzeni, wskazującego na realne granice dopuszczalności ruchu w sieci. W szczególności, należy uznawać, iż o bezprawności działań w cyberprzestrzeni winien świadczyć brak faktycznych praw do przetwarzania (otwierania, modyfikowania, kopiowania – choćby częściowego) danego zasobu, co wcale jednak nie musi być odzwierciedlane w programowo-sprzętowych systemach bezpieczeństwa. Tak samo, jak nikt nie ma prawa wchodzić do mieszkania drugiej

osoby, niezależnie od faktu zamknięcia przez nią zamka w drzwiach, czy też przywłaszczania ruchomości, która nie jest jednoznacznie oznakowana, jako porzucona - tak też bezprawność uzyskania dostępu do cudzych zasobów komputerowych nie powinna być oceniana przez pryzmat zastosowania w penetrowanym systemie szczególnych zasad bezpieczeństwa. Należy w tym miejscu podkreślić, iż tak jak w przypadku mienia fizycznego – zarówno ruchomości, jak i nieruchomości, również i w cyberprzestrzeni brak jest jakichkolwiek obowiązków zabezpieczania swojej własności oraz posiadanych odnośnych rozwiązań systemowych. W istocie, brak jest nawet jakichkolwiek rozwiązań prawnych, które nakładałyby obowiązek zabezpieczania własnej sieci oraz posiadanego dostępu do Internetu. Warto podkreślić, iż brak takich zabezpieczeń może skutkować wykorzystaniem danej sieci do wykonania ataku przez osoby trzecie przy zachowaniu atrybucji działań do posiadacza niechronionego łącza,

- pozostając w powyższym kontekście, należy również podnieść, iż karalność uzyskiwania bezprawnego dostępu do systemu winna być rozumiana na gruncie przepisów karnych bez ograniczenia do dostępu do określonych danych przetwarzanych w tym systemie. Uzyskanie dostępu do systemu może bowiem polegać wyłącznie na dostaniu się np. do jego części konfiguracyjnej. Tego typu wejście nie musi konstytuować pozyskania jakichkolwiek informacji, czy też nawet wiązać się z wprowadzeniem jakichkolwiek nieuprawnionych zmian, ograniczając się jedynie do rozpoznania możliwości dalszych prowadzenia działań bezprawnych. Z uwagi na swoją doniosłość dla bezpieczeństwa użytkowników sieci tego typu operacje winny jednak podlegać jednoznacznej penalizacji karnej, w przypadku której przedmiotem ochrony nie będzie jednak ani tajemnica korespondencji, czy też prawo do swobodnego przetwarzania posiadanych informacji oraz danych – zaś samo bezpieczeństwo systemów teleinformatycznych, rozumiane jako suwerenna wartość.

Wnioski oraz postulaty w zakresie transpozycji czynności procesowych do obszaru cyberprzestrzeni.

Bezpośrednią konsekwencją uwag zebranych wyżej w punktach I i II - odnoszących się do specyfiki cyberprzestrzeni, jako nowego obszaru aktywności ludzkiej oraz niejako narzucanych przez tę specyfikę cech szczególnych samej cyberprzestępczości

– jest ostatecznie przedstawienie koniecznych zmian w sposobie pojmowania czynności procesowych realizowanych w obszarze domeny cyfrowej. Czynności te, w sposób oczywisty, muszą bowiem ulegać analogicznym „odkształceniom" interpretacyjnym warunkowanym przez cechy szczególne zjawiska, którego wprost dotyczą, ujmując je jako swój przedmiot. Mając na uwadze zachodzącą w sieciach komputerowych „wirtualizację" rzeczywistości, szczególną (wyłącznie cyfrową) formę, jaką przybierają dowody aktywności jej użytkowników, a także nowe możliwości i wyzwania, jakie niesie ze sobą realizacja czynności wykrywczych oraz dowodowych w systemach teleinformatycznych (m.in. związanych bezpośrednio z koniecznością pracy na danych komputerowych), w tym także uwzględniając problematykę czynności realizowanych na odległość (*on-line)* - w przedmiotowym zakresie należy sformułować następujące wnioski:

- obowiązujące przepisy regulujące zasady podejmowania czynności procesowych przez uprawnione podmioty tworzone były jednoznacznie z myślą o działaniach konwencjonalnych, podejmowanych fizycznie, w otaczającej nas rzeczywistości, wobec osób oraz namacalnych przedmiotów (narzędzi, dokumentów, fizycznych nośników danych). Z uwagi na specyfikę obszaru cyberprzestrzeni, zasady te nie odpowiadają jednak wymogom pracy z zasobami cyberprzestrzeni, które pozostają niematerialne, zaś wyrażają się zawsze w postaci danych komputerowych (niezależnie od rodzaju treści, które dane te ucieleśniają). Co istotne – dane zapisane w wielu różnych postaciach (np. magnetycznie na dyskach twardych, optycznie na płytach) stanowią wyłącznie swoisty substrat reprezentowanych treści oraz działań, będąc w istocie jedyną materią cyfrowej tkanki cyberprzestrzeni,

- ponieważ podstawowym dowodem popełnienia cyberprzestępstwa są zasoby występujące w postaci elektronicznej (cyfrowej), za punkt wyjścia dla rozwoju prawa procesowego w zakresie działania w cyberprzestrzeni należy bezwzględnie przyjąć wprowadzenie definicji legalnej dowodu elektronicznego. Dowodem tym powinny w szczególności pozostawać wszelkie dane wykazujące powiązanie działania systemu atakującego z negatywnym, bezprawnym skutkiem występującym po stronie systemu atakowanego. W ocenie autora niniejszej pracy, dowody elektroniczne powinny jednocześnie odnosić się do zasobów, jak i samych działań realizowanych wewnątrz obszaru cyberprzestrzeni, reprezentując przede wszystkim zapis ruchu sieciowego, historię wydawanych poleceń oraz wpisywanych komend, a także działania sieciowe

mogące wskazywać na fakt przygotowywania przestępstwa (np. zapis o skanowaniu portów). Definicja legalna dowodu powinna wymagać zachowania autentyczności dowodu (cecha stanowiąca w języku informatycznym o oryginalności materiału, czy też braku jakichkolwiek jego modyfikacji) odrywając się jednocześnie od kwestii liczby egzemplarzy, w których danych zasób został wykonany (zapis jednego materiału pobrany z różnych miejsc stanowi w dalszym ciągu jego idealną kopię, z uwagi na atrybut bezstratności procesu powielania danych informatycznych),

- rozumianych w powyższy sposób dowodów elektronicznych w żadnej mierze nie można odrywać od kwestii dowodzenia działania określonego sprawcy, które to działanie – zawsze przybiera postać fizycznego działania człowieka. W tym kontekście, dowody elektroniczne można przyrównać do śladów na jezdni po wydarzeniu drogowym, które dla osądzenia określonej osoby, muszą jednak zostać uzupełnione dowodami działania lub zaniechania oznaczonego sprawcy – kierowcy pojazdu. W przypadku zwalczania cyberprzestęczości, konieczne jest zatem wypracowanie jednolitych zasad prowadzenia tzw. atrybucji określonego działania do ściśle zdefiniowanego, zindywidualizowanego użytkownika systemu. Działania te wymagają w szczególności odpowiedniej korelacji czynności procesowych podejmowanych w obszarze cyberprzestrzeni, jak również konwencjonalnych czynności dowodowych,

- ujęcie prawne dowodu elektronicznego wymaga jasnego oraz precyzyjnego wyznaczenia granic prawnych dla możliwości pozyskiwania takich dowodów przez uprawnione podmioty. W szczególności konieczne jest rozstrzygnięcie kwestii wartości dowodowej materiałów pozyskiwanych za pośrednictwem sieci, to jest w ramach czynności wykonywanych zdalnie *(on-line)* oraz bez udziału osób innych niż sami funkcjonariusze. W ocenie autora – pozyskane tak materiały, pod warunkiem zastosowania odpowiednich rozwiązań sprzętowo-programowych (w szczególności zabezpieczających pozyskiwany materiał przed możliwością dokonania w nim jakichkolwiek modyfikacji), winny posiadać samodzielny walor dowodowy, nie wymagając dokonywania jakichkolwiek transpozycji procesowych np. w ramach przesłuchiwania w charakterze świadka funkcjonariusza wykonującego *on-line* kopię materiału o charakterze bezprawnym, celem jego zabezpieczenia. Rozwiązanie to wymaga jednak jednoznacznego uregulowania kompetencji organów ścigania do działania w cyberprzestrzeni, celem wyeliminowania możliwości dokonywania

nadużyć zarysowujących się na tle coraz to kolejnych doniesień prasowych o systemach inwigilacji państwowej w cyberprzestrzeni,

- uzupełniając powyższe uwagi dot. procesów pozyskiwania dowodów elektronicznych należy także zwrócić uwagę na zasadność uregulowania prawnego kompetencji organów ścigania w zakresie prowadzenia dekryptażu ewentualnie zaszyfrowanych materiałów dowodowych lub też prawa tychże organów do żądania wydania haseł, kodów lub innych analogicznych środków lub narzędzi niezbędnych do otwarcia zabezpieczonych danych. Należy zaznaczyć, iż z uwagi na powszechną dostępność darmowych, programowych rozwiązań szyfrujących (rozwiązania tego typu można pobrać z legalnie działających stron internetowych), których używanie nie wymaga w dodatku stosowania jakiejkolwiek wiedzy specjalistycznej (oprogramowanie tego typu posiada najczęściej prosty interfejs graficzny oraz tzw. *wizard* procesu szyfrowania danych – umożliwiający proste skonfigurowanie programu do szyfrowania bądź to wyłącznie danych wybranych przez użytkownika bądź też szyfrowanie na bieżąco całej zawartości komputera) – problematyka pozyskiwania rzeczywistego dostępu do dowodów elektronicznych staje się obecnie coraz bardziej utrudniona. Uzupełniając powyższe o wskazanie na rosnącą wielkość przetwarzanych obecnie na co dzień plików (wskaźnik ten posiada bezpośredni wpływ na czas potrzebny do rozszyfrowania zasobu), należy wręcz antycypować, iż uzyskiwanie przez organy ścigania dostępu do zaszyfrowanych plików może w niedalekiej przyszłości stać się uniemożliwione. W tym kontekście, za w pełni zasadne należy uznać wprowadzenie mechanizmów procesowych, które umożliwiałyby pozyskiwanie stosownych haseł ze wszelkich dostępnych źródeł, w tym przede wszystkim z zastosowaniem technik informatycznych nastawionych na ich łamanie lub omijanie, z przyjęciem ryzyka iż proces ten może wiązać się fragmentaryzacją pozyskiwanych dowodów (specyfika procesu dekryptażu może nie pozwalać na dostęp do całej zawartości odkodowywanych treści). Dalszej analizy prawnej wymaga także kwestia oceny dopuszczalności stosowania w procesie karnym typowo ofensywnych, aktywnych metod pozyskiwania dowodów elektronicznych np. w drodze instalowania w sposób niejawny oprogramowania kontrolnego, pozwalającego pozyskiwać określone materiały jeszcze przed ich zaszyfrowaniem, choć problematyka ta wywoływała do tej pory nie tylko liczne spory prawne, ale także stanowczy opór opinii publicznej, jako rozwiązanie nadmiernie ingerujące w prawa i swobody

obywateli. Wydaje się także iż rozwiązaniem zupełnie nieakceptowalnym byłoby natomiast nakładanie obowiązku udostępniania haseł na samego oskarżonego, który już w myśl postanowień obowiązującej Konstytucji Rzeczypospolitej Polski, nie posiada obowiązków współpracy z organami ścigania w zakresie dowodzenia swojej winy,

- specyfika cyberprzestrzeni nakazuje odrębne uregulowanie zasad oraz metod prowadzenia czynności procesowych wykonywanych w obszarze domeny cyfrowej, w szczególności zaś czynności przeszukania systemu oraz zatrzymania danych. W pierwszej kolejności, za niezbędne należy uznać określenie zasad udziału w tych czynnościach osób dysponujących systemem oraz wyznaczenie zakresu ich obowiązków prawnych (np. udostępnienia haseł dostępowych przez administratora). Po drugie, przepisy procesowe winny określać choćby zgrubnie metodykę poszukiwania oraz zatrzymywania określonych zasobów, mając na uwadze zarówno konieczność zapewnienia poprawnego biegu postępowania, jak również prawnie chronione interesy obywateli – nierzadko fizyczne zabezpieczenie komputerów przedsiębiorstwa może spowodować totalny paraliż jego działania, nie będąc jednocześnie niezbędne z punktu widzenia technicznego. Z drugiej strony – konieczność wyłączenia danego systemu może wynikać także z powodu możliwości wystąpienia dalszych infekcji lub zautomatyzowanych ataków realizowanych przez określony system. Po trzecie też – przeszukiwanie oraz zatrzymywanie zasobów cyberprzestrzeni winno zostać obwarowane prawnym wymogiem zapewnienia autentyczności materiału dowodowego występującego w postaci elektronicznej,

- przyszłe regulacje odnoszące się do prowadzenia czynności procesowych w cyberprzestrzeni winny charakteryzować te czynności, jako działania techniczne, wykonywane wewnątrz systemów, nie zaś wobec nich. Ta istotna dystynkcja ma na celu wskazanie, że poddany czynnościom system nie musi stanowić sam w sobie ich przedmiotu, zaś może być wykorzystywany jako swoiste narzędzie np. do pozyskania nagranych w nim danych lub też ustalenia występowania określonych cech systemu (np. czy ten posiada zabezpieczenia, czy też możliwe było skorzystanie z niego przez osobę postronną bez przełamywania, czy nawet omijania dowolnych środków ochrony),

- ostatecznie, powodzenie realizacji celów procesu karnego w sprawach o cyberprzestępstwa uzależnione jest w ogromnej mierze od skuteczności współpracy międzynarodowej organów ścigania, właściwych do podejmowania działań w przedmiotowym zakresie. Z uwagi na globalny zasięg cyberprzestrzeni – oraz powodowany tym transgraniczny charakter działalności cyberprzestępców, efektywne zwalczanie poruszanego zjawiska przestępnego wymaga wypracowania odformalizowanych procedur wymiany informacji na temat sieciowych działań użytkowników - sprawców ataków teleinformatycznych. Należy wyrazić pogląd, iż w świetle stosowanych metod anonimizacji ruchu sieciowego, czy też jego przekierowywania przez węzły teleinformatyczne ulokowane na terytorium wielu państw – pojedynczy kraj, działający w osamotnieniu nie jest w stanie stawić czoła nowoczesnym zagrożeniom płynącym ze świata cyberprzestrzeni.

BIBLIOGRAFIA

1. Adamski A., Cyberprzestępczość - aspekty prawne i kryminologiczne, Studia Prawnicze, Nr 4 z 2005 r., INP PAN, Warszawa 2005.
2. Adamski A., Prawo karne komputerowe, Wydawnictwo CH Beck, Warszawa 2000.
3. Adamski A., Przestępczość w cyberprzestrzeni, prawne środki przeciwdziałania zjawiska w Polsce na tle projektu konwencji Rady Europy, Dom Organizatora, Toruń 2011.
4. Aldrich R. W., *Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime*, USAF INSS *Occasional Paper 32*, USA – Colorado 2002.
5. Ambrosi A., Peugeot V., Pimienta D., Word Matters*: multicultural perspectives on information societies, C & F Editions*, Francja - Caen 2005.
6. Artymiak G., Sobolewski Z., Wolters Kluwer, Warszawa 2007.
7. Balkin J. M., Grimmelmann J., Katz E., Kozlovski N., Wagman S., Zarsky T., *Cybercrime: digital cops in a networked environment*, New York University Press, Nowy Jork 2007.
8. Bednarek J., Teoretyczne i metodologiczne podstawy badań nad człowiekiem w cyberprzestrzeni, Cyberświat: możliwości i zagrożenia, pod red.: Bednarek J., Andrzejewska A., Wydawnictwo Akademickie Żak, Warszawa 2009.
9. Bequai A., *Computer Crime*, Lexington Books, USA 1978.
10. Bequai A., *Technocrimes*, Lexington Mass, 1987.
11. Bethke B., *Cyberpunk*, Wyd. Bruce Bethke, USA 1984.
12. Błachut J., Dokument jako przedmiot ochrony prawnokarnej, Lex, Warszawa 2011.
13. Bojańczyk A., Glosa do wyroku Sądu Najwyższego z 10 maja 2002 r., WA 22/02, Palestra 2003, Nr 7 – 8, Warszawa 2003.
14. Bojarski T., Michalska-Warias A., Piórkowska-Flieger J., Szwarczyk M., Kodeks karny. Komentarz, LexisNexis, wyd. 3, Warszawa 2009.
15. Brown C., *Computer Evidence: Collection and Preservation*, Charles River Media, USA 2009.
16. Bryant R., Bryant S., *Policing Digital Crime*, Wyd. Ashgate, Anglia 2014.
17. Castells M., Społeczeństwo sieci, Wydawnictwo Naukowe PWN, Warszawa 2010.
18. Casey E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Elsevier, USA - Massachusetts 2011.
19. Chauvin T., Stawecki T., Winczorek P., Wstęp do prawoznawstwa, C. H. Beck, Warszawa 2011, wyd. 6.
20. Cross M., Littlejohn Shinder D., *Scene of the Cybercrime*, Syngress, USA - Burlington 2008.
21. Dahl M., *Computer Evidence*, Capstone 2004.
22. Dobrowolski G., Nawarecki E., Dajda J., Byrski A., Kisiel-Drohinicki M., *Scenario-Driven Systems for Open Source Intelligence*, *Multimedia Communications, Services and Security*, CCIS *vol*. 287, Springer 2012.
23. Dobrowolski G., Nawarecki E., Sytuacje kryzysowe w systemach agentowych, Automatyka 2005, tom 9, zeszyt 1-2, Kraków 2005.
24. Dobrzeniecki K., Prawo a etos cyberprzestrzeni, Wyd. Adam Marszałek, Toruń 2004.
25. Doktorowicz K., Europejski model społeczeństwa informacyjnego. Polityczna strategia Unii Europejskiej w kontekście globalnych problemów wieku informacji, Wyd. Uniwersytetu Śląskiego, Katowice 2005.
26. Doyle C., *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, *Congressional Research Service*.

Opracowanie dostępne na stronie internetowej pod adresem: http://www.fas.org/sgp/crs/misc/97-1025.pdf.
27. Duff L., Gardiner S., *Compuer Crime in the Global Village: Strategies for Control and Regulation - in Defence of the Hacker* [w:] D. S. Wall, *Cyberspace Crime*, Wyd. Ashgate, Anglia 2003.
28. Eck W., *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*, praca dostępna na stronie internetowej pod adresem: http://cryptome.org/emr.pdf.
29. Erkkonen H., Larsson J., *Anonymous Networks*. Opracowanie dostępne na stronie internetowej Uniwersytetu Chalmers, pod adresem: http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/Files/onion_routing.pdf.
30. Farha A., *IP Spoofing, The Internet Protocol Journal, Vol*. 10, Nr 4, Wyd. CISCO, San Jose USA 2007.
31. Filipkowski W. (pod red.), Pływaczewski E. W. (pod red.), Rau Z. (pod red.), Przestępczość w XXI wieku - zapobieganie i zwalczanie. Problemy technologiczno-informatyczne, Wolters Kluwer, Wyd. I, 2015.
32. Fischer B., Przestępstwa komputerowe i ochrona informacji. Aspekty prawno kryminalistyczne, Zakamycze, Kraków 2000.
33. Gaberle A., Dowody w sądowym procesie karnym, Oficyna, wyd. 2, Warszawa 2010.
34. Gahtan A. M., *Electronic Evidence*, Carswell 1999.
35. Geist M., *Is There a There There? Toward greater certainty for Internet Jurisdiction*, tekst opracowania dostępny na stronie internetowej pod adresem: http://www.law.berkeley.edu/journals/btlj/articles/vol16/geist/geist.pdf.
36. Galewska E., Okoń Z., Ożóg M., Szostek D., Świerczyński M., Trybuchowska E., *Cyber Law in Poland*, Wolters Kluwer, Holandia 2011.
37. Gibson W., Neuromancer, *Ace Books*, Nowy York 1984.
38. Giezek J., Kodeks karny. Część szczególna. Komentarz, pod red. Giezek J., Gruszecka D., Kłączyńska N., Łabuda G., Muszyńska A., Razowski T., LEX 2014.
39. Goldsmith J. L., *Against* Cyberanarchy, *University of Chicago Law* Review *Fall 1998*, Chicago 1998.
40. Goodman M., *Making Computer Crime Count*, *FBI Law Enforcement Biulettin*, sierpień 2001. Biuletyn dostępny na stronie internetowej pod adresem: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2001-pdfs/aug01leb.pdf.
41. Goodman M., Brenner S., *The Emerging Consensus on Criminal Conduct in Cyberspace*. Opracowanie dostępne na stronie internetowej pod adresem: http://ijlit.oxfordjournals.org/content/10/2/139.citation).
42. Grabowski R., Wpływ Internetu na ewolucję państwa i prawa, praca pod red. R. Grabowskiego, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2008.
43. Gragido W., Pirc J., *Cybercrime and Espionage. An analysis of Subversive Multivector Threats*, Elsevier, USA - Rockland 2011.
44. Grzegorczyk T., Dowody w procesie karnym, Wydawnictwo Prawnicze, Warszawa 1998.
45. Grzegorczyk T., Tylman J., Polskie postępowanie karne, Lexis Nexis, wyd. 8, Warszawa 2011.
46. Hanausek T., Kryminalistyka, Zakamycze 2000.
47. Hollinger R. C., *Crime, Deviance and the Computer*, The International Library of Criminology, Criminal Justice and Penology, Aldershot, Darthmouth 1997.
48. Hołyst B., Pomykała J., Cyberprzestępczość, ochrona informacji i kryptologia, Prokuratura i Prawo 2011, Nr 1, Kraków 2011.

49. Jankowski J., Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa, Difin, Warszawa 2012.
50. Jankowski J., *Technological Destabilization of Law* [w]: W. Cyrul, *Information Technology of Law*, Wyd. Uniwersytetu Jagiellońskiego, Kraków 2014.
51. Jasiński W., Nadużycia w przedsiębiorstwie – przeciwdziałania i wykrywanie, Poltext, Warszawa 2013.
52. Johnson D. R., Post D. G., *Law And Borders: The Rise of Law in Cyberspace*, 48 Stanford Law Review 1367 (1996).
53. Joseph G., *Modern Visual Evidence*, American Lawyer Media, Nowy Jork 1984
54. Kalitowski M., Kodeks karny. Komentarz, Wielkie Komentarze, pod red. M. Filara, LexisNexis, wyd. 2, Warszawa 2010.
55. Kania A., Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni, *e-biuletyn* CBKE 1/2009, Wrocław 2009. Tekst opracowania dostępny jest na stronie internetowej pod adresem: http://bibliotekacyfrowa.pl/Content/34350/Oszustwo_komputerowe.pdf.
56. Kelman M., *A Guide to Critical Legal Studies, Harvard University Press,* Londyn 1987.
57. Kevelson R., *The Law as a System of Signs, Plenum Press,* Nowy Jork 1988.
58. Kliś M., Przestępczość w Internecie. Zagadnienia podstawowe, Czasopismo Prawa Karnego i Nauk Penalnych, Wydawnictwo Polska Akademia Umiejętności, Kraków 2000.
59. Kasprzak W., Ślady cyfrowe. Studium prawno-kryminalistyczne, Difin, Warszawa 2015.
60. Kojder A., Godność i siła prawa, Oficyna Naukowa, Warszawa 2001.
61. Kołodziej M., Internet rzeczy, nowe spojrzenie na ochronę prywatności, w: Kosiński J., Przestępczość teleinformatyczna 2015, Szczytno 2015.
62. Kosmaty P., Podsłuch komputerowy. Zarys problematyki, Prokurator 2008, Nr 4, Poznań 2008.
63. Kosiński J. (pod red.), Przestępczość teleinformatyczna 2015, Szczytno 2015.
64. Kosiński J. (pod red.), Przestępczość teleinformatyczna: IX seminarium naukowe: materiały seminaryjne, WSPol, Szczytno 2006.
65. Kosiński J. (pod red.), Przestępczość teleinformatyczna: X seminarium naukowe: materiały poseminaryjne, WSPol, Szczytno 2007.
66. Kosiński J. (pod red.), Szafrański J. (pod red.), Przestępczość teleinformatyczna: XI seminarium naukowe: materiały poseminaryjne, WSPol, Szczytno 2008.
67. Kozerska E., Sadowski P., Szymański A., Ze studiów nad tradycją prawa, Difin, Warszawa 2012.
68. Kozłowska-Kalisz P., Kodeks karny. Komentarz, pod red. Mozgawa M., Budyn-Kulik M., Kozłowska-Kalisz P., Kulik M., WK, 2015, system LEX.
69. Kunicka-Michalska B., Kodeks Karny, Duże Komentarze Becka Tom II, pod red. prof. A. Wąska i prof. R. Zawłockiego, Warszawa 2010
70. Kunicka-Michalska B., Pornografia i wykorzystywanie nieletnich w Internecie. Regulacje polskiego Kodeksu karnego, Studia Prawnicze, Zeszyt 4 (166) 2005 r., Instytut Nauk Prawnych PAN, Warszawa 2006.
71. Lach A., Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia teoretyczne i praktyczne, *e-biuletyn* CBKE 2/2004, Wrocław 2004.
72. Lach A., Dowody elektroniczne w procesie karnym, Towarzystwo Naukowe Organizacji i Kierownictwa, Dom Organizatora, Toruń 2004.
73. Lach A., Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego, Prokuratura i Prawo 2003, Nr 10, Kraków 2003.

74. Lach A., Kodeks karny. Komentarz, WK, 2016, system LEX.
75. Lach A., Prawa i obowiązki dysponentów i użytkowników systemu informatycznego w związku z jego przeszukaniem i zatrzymaniem danych. Pełny tekst opracowania dostępny na stronie internetowej pod adresem: http://www.secure.edu.pl/historia/2005/docs/26.10/07_lach/lach-r.pdf.
76. Lach A., Przeszukanie na odległość systemu informatycznego, Prokuratura i Prawo 2011. Tekst opracowania dostępny na stronie internetowej pod adresem: http://prawo.uni.wroc.pl/pliki/13373.
77. Lange M. C. S., Nimsger K. M., *Electronic Evidence and Discovery: What Every Lawyer Should Know*, Wydawnictwo American Bar Association, Chicago 2009.
78. Lovet G., *Fighting Cybercrime: Technical, Juridical and Ethical Challenges*. Opracowanie dostępne na stronie internetowej pod adresem: http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf.
79. MacDonald Newhook C., *Cybersquatters Beware!: Insiders' Tips on Winning Domain Name Disputes*, wyd. *McGraw-Hill Ryerson*, Londyn 2002.
80. Małycha S. (wstęp), Informatyka śledcza okiem prawników, materiały Mediarecovery, Media Sp. z o.o., Warszawa 2014, opracowanie dostępne na stronie internetowej pod adresem: https://magazyn.mediarecovery.pl/wp-content/uploads/prawnicy.pdf.
81. Marcella A. J., Guillossou F., *Cyber Forensics: From Data to Digital Evidence*, Wydawnictwo John Wiley & Sons, New Jersey 2012.
82. Maroń G., Zasady prawa. Pojmowanie i typologie a rola w wykładni prawa i orzecznictwie konstytucyjnym, Wyd. Ars boni et aequi, Poznań 2011.
83. Marshall Jarrett H., Bailie M. W., Hagen E., Eltringham S., *Prosecuting Computer Crimes, Office of Legal Education Executive Office for United States Attorneys* - wydawnictwo Ministerstwa Sprawiedliwości USA (Department of Justice), Washington DC 2010.
84. Mazur M., Cybernetyczna teoria układów samodzielnych, PWN, Warszawa 1966.
85. Mitnick K., Sztuka podstępu, Helion, Gliwice 2002.
86. Misztal-Konecka J., Tylec G., Ewolucja prawa polskiego pod wpływem technologii informatycznych, Wydawnictwo KUL, Lublin 2012.
87. Mohammed Kadir R., *The Scope and the Nature of Computer Crimes Statutes – A Critical Comparative Study.* Opracowanie dostępne na stronie internetowej pod adresem: http://www.germanlawjournal.com/index.php?pageID=11&artID=1259.
88. Moore E. S. *Cyber-jurisdiction, Virginia Lawyer April 2002*, USA 2002.
89. Nawarecki E., Dobrowolski G., Byrski A., Kisiel-Drochnicki M., Agent-Based Integration of Data Acquired from Heterogenous Sources, cyfrowa biblioteka IEEE.
90. Nowak T., Dowód z dokumentu w polski procesie karnym, Poznań 1994.
91. Ottis R., Lorents P., *Cyberspace: Definition and Implications*, Cooperative Cyber Defence Centre of Excellence ulokowane w Tallinie. Opracowanie dostępne na stronie internetowej CCDCOE pod adresem: http://www.ccdcoe.org/205.html.
92. Papińska-Kacperek J. (red.), Społeczeństwo Informacyjne, Wydawnictwo Naukowe PWN, Warszawa 2008.
93. Parker D. B., *Crime by Computer*, Scribner, Nowy Jork 1976.
94. Pawelec K. J., Proces dowodzenia w postępowaniu karnym, Lexis Nexis, Warszawa 2010.
95. Pływaczewski E. W., Zapobieganie przestępczości i sprawiedliwość karna. XII Kongres Organizacji Narodów Zjednoczonych (Salwador, Brazylia, 12-19 IV 2010), Państwo i Prawo 2010, z. 10, s. 133 i nast.

96. Pływaczewski E. W., Współczesne tendencje przestępczości i kierunki jej przeciwdziałania z perspektywy XII Kongresu ONZ, w: Teoretyczne i praktyczne problemy współczesnego prawa karnego, Księga Jubileuszowa dedykowana Profesorowi Tadeuszowi Bojarskiemu, A. Michalska-Warias, I Nowikowski, J. Piórkowska-Flieger, UMCS, Lublin 2010.
97. Podraza A., Potakowski P., Wiak K., Cyberterroryzm zagrożeniem XXI wieku, Difin, Warszawa 2013.
98. Podrecki P., Okoń Z., Litwiński P., Świerczyński M., Targosz T., Smycz M., Kasprzycki D., Prawo Internetu, Lexis Nexis, wyd. 2, Warszawa 2007.
99. Polański P., Prawo Internetu, C. H. Beck, Warszawa 2008.
100. Pomarański M., Haktywizm jako ruch protestu XXI wieku, w: M. Marczewska-Rytko, Haktywizm. Cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja, Wyd. UMCS, Lublin 2014.
101. KUL, Lublin 2013.
102. Reyes A., *Cyber Crime Investigations*, Elsevier, USA - Rockland, 2007.
103. Reyes A., Wiles J., *The Best Damn Cybercrime and Digital Forensics Book Period*, Syngress, USA - Burlington 2007.
104. Sakowicz A., Kodeks karny - część szczególna, tom 2, pod red. Królikowski M., Zawłocki R., Warszawa 2013.
105. Potrzeszcz J., Bezpieczeństwo prawne z perspektywy filozofii prawa, Wydawnictwo Schjolberg S., *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*. Opracowanie dostępne na stronie internetowej pod adresem: www.cybercrimelaw.net/documents/cybercrime_history.pdf).
106. Sieber U., *Computercriminalitat und Strafrecht*, Heymann 1977.
107. Sieber U., Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka, Przegląd Policyjny, Nr 3/95, Szczytno 1995.
108. Singh A. w: *Ascertaining Cyber Jurisdiction in Cyber Space: Jurisprudential Understanding and a Comparative Analysis, Social Science Electronic Publishing*, USA 2009.
109. Siwicki M., Cyberprzestępczość, C. H. Beck, Warszawa 2013.
110. Stawecki T., Winczorek P., Wstęp do prawoznawstwa, Wydawnictwo CH Beck, Warszawa 2003.
111. Suchorzewska A., Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem, Oficyna a Wolters Kluwer Business, Warszawa 2010.
112. Takemura N., *Crime-and-Punishment-Related Information and Its Control in Postmodern Society: Fundamental Understanding on Control Mode of Information*, w: Przegląd Policyjny Nr 1 (61) 2001.
113. Taracha A., Czynności operacyjno rozpoznawcze, aspekty kryminalistyczne i prawnodowodowe, Wydawnictwo UMCS, Lublin 2006.
114. Tęcz-Paciorek A., Zasada domniemania niewinności w polskim procesie karnym, Lex, Warszawa 2012.
115. Thomas D., Loader B. D., *Cybercrime. Law enforcement, security and surveillance in the information age*, Wyd. Routledge, Londyn 2000.
116. Trejderowski T., Kradzież tożsamości. Terroryzm informatyczny, Eneteia, Warszawa 2013.
117. Vuagnoux M., Pasini S., *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*. Opracowanie dostępne na stronie internetowej pod adresem: http://www.usenix.org/event/sec09/tech/full_papers/sec09_attacks.pdf.
118. Waglowski P., Prawo w sieci. Zarys Regulacji Internetu, Wydawnictwo Helion 2005.

119. Waltoś S., Proces karny. Zarys systemu, Lexis Nexis, wyd. 10, Warszawa 2009.
120. Wiener N., *Cybernetics: Or Control and Communication in the Animal and the Machine*, John Wiley & Sons, New York 1948.
121. Wilding E., *Computer Evidence: A Forensic Investigations Handbook,* Londyn 1997.
122. Wróbel W., Kodeks karny, Część szczególna. Tom II. Komentarz do art. 117-277 k.k., pod red. A. Zolla, Barczak-Oplustil A., Bielski M., Bogdan G., Ćwiąkalski Z., Dąbrowska-Kardas M., Majewski J., Raglewski J., Szewczyk M., Wróbel M., LEX 2013.
123. Zelek M., Przeszukanie urządzenia zawierającego dane informatyczne lub systemu informatycznego w świetle polskiego procesu karnego. Tekst opracowania dostępny na stronie internetowej pod adresem: http://www.edukacjaprawnicza.pl /aktualnosci/a/pokaz/c/aktualnosc/art/przeszukanie-urzadzenia-zawierajacego-dane-informatyczne-lub-systemu-informatycznego-w-swietle-polskiego-procesu-karnego.html.